BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 1/2026

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

"CAROL I" NATIONAL DEFENCE UNIVERSITY PUBLISHING HOUSE
BUCHAREST, 2026

Scientific Reviewers

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. 1/2026

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY
https://buletinul.unap.ro/index.php/en/

A Narrative Intelligence Approach to European Climate Change and Migration Policy: a Case Study of the Sahel

Colonel (Retired) William F. LYONS Jr., JD*
Diane M. ZORRI, Ph.D.*
*Vice President for Distance Education, Norwich University, Northfield, Vermont, USA
e-mail: WLyons@norwich.edu
https://orcid.org/0000-0001-5953-8620
**Academic Director, Department of Strategic Studies, College of Graduate and Continuing Studies, Norwich University, Northfield, Vermont, USA
e-mail: DZorri@norwich.edu
https://orcid.org/0000-0001-7294-325X

Abstract

The application of narrative intelligence to the climate, migration, and terrorism nexus in the Sahel reveals critical insights that are often obscured by traditional analytical approaches. Narrative intelligence, understood as the systematic analysis of stories, symbols, and meaning-making processes, exposes the emotional and cognitive dimensions that underpin climate-related instability in this fragile region. This study demonstrates that extremist organizations across the Sahel strategically exploit narratives of environmental injustice, displacement, and marginalization to recruit members and legitimize violence. It also shows that competing portrayals of climate migrants, whether as vulnerable populations deserving protection or as potential security threats requiring containment, shape national and regional policy responses that can either mitigate or intensify existing tensions. Moreover, the absence of coherent and empowering narratives surrounding climate adaptation and livelihood resilience creates ideological vacuums that violent extremist movements are quick to fill. By integrating narrative intelligence into security and policy assessments, this study argues that reframing climate migration through inclusive and resilience-oriented narratives offers a powerful form of strategic communication. Such an approach can reduce recruitment potential, promote more coherent governance strategies, and strengthen societal resilience across the Sahel in the face of accelerating climate and security challenges. Using Open Source Intelligence (OSINT) tools, this article pursues three interrelated objectives: to identify the dominant narrative frameworks shaping policy and public discourse on the climate–migration–terrorism nexus as it pertains to the Sahel and Europe; examine how those narratives structure particular policy responses; and assess the implications of competing and convergent narratives for counterterrorism and climate adaptation strategy.

Keywords:
Climate Change; Sahel; Migration; Terrorism; Europe; Narrative Intelligence.

Article info
Received: 22 November 2025; Revised: 16 December 2025; Accepted: 28 January 2026; Available online: 08 April 2026

Citation: Lyons, W.F., and D.M. Zorri. 2026. "A Narrative Intelligence Approach to European Climate Change and Migration Policy: a Case Study of the Sahel." *Bulletin of "Carol I" National Defence University*, 15(1): 7-28. https://doi.org/10.53477/2284-9378-26-01

Introduction

The intersection of climate change, migration, and terrorism represents one of the most complex security challenges of the twenty-first century, yet traditional analytical frameworks often fail to capture the intricate human dimensions that drive these interconnected phenomena (Reyer et al. 2017; Torres and Casey 2017). Quantitative approaches have long dominated policy research in this domain, focusing primarily on statistical correlations between environmental stressors, population movements, and conflict incidents (Buhaug 2015; Schleussner et al. 2016). While such methods offer valuable empirical insights, they frequently overlook the critical role that identity formation and collective narratives play in shaping individual and group responses to environmental displacement (Adger et al. 2014; Mortreux and Barnett 2017).

This article pursues three interrelated objectives. First, it seeks to identify the dominant narrative frameworks shaping policy and public discourse on the climate–migration–terrorism nexus as it pertains to the Sahel and Europe. Second, it examines how those narratives structure problem definition, assign responsibility, and privilege particular policy responses while marginalizing others. Third, it assesses the implications of competing and convergent narratives for counterterrorism and climate adaptation strategy, with particular attention to whether current EU policy approaches engage seriously with the narrative foundations of extremist appeal in contexts of environmental stress. The article employs a qualitative, narrative intelligence framework. This approach draws on two foundational traditions: Goffman's (1974) frame analysis, which established how individuals and institutions organize experience through interpretive schemas, and Entman's (1993) framing theory, which demonstrated how the selection and salience of information in texts shape problem definition, causal attribution, and policy prescription.

This paper contends that incorporating narrative intelligence into the analytical toolkit is essential for states seeking to develop more effective and sustainable responses to the security challenges arising from climate-induced migration. By examining the stories that shape how different actors interpret and respond to environmental displacement, we can better understand the conditions under which climate migration becomes a pathway to radicalization and identify intervention points for more targeted prevention strategies (Rüttinger et al. 2015). Rather than treating narratives as secondary or peripheral phenomena to be explained away, this approach positions them as central mechanisms through which environmental change translates into social and political outcomes (O'Brien and Barnett 2013; Pelling and High 2013).

Climate-induced migration unfolds within specific cultural, political, and social contexts in which competing narratives about causation, responsibility, and legitimate response shape how communities interpret their experiences of

displacement (Hunter et al. 2015; McMichael et al. 2012). These narratives influence not only how displaced populations understand their predicament but also how host communities, governments, and extremist organizations frame and respond to migration flows (Boas 2015; Farbotko and McMichael 2019). When conventional analytical methods treat these human stories as mere background noise to be controlled statistically, they miss the fundamental mechanisms through which environmental stress transforms into social tension and, in some cases, violent extremism (Ide 2018; Koubi et al. 2018). This dynamic is visible in climate and violence-induced migration from Africa to Europe, where illicit migratory flows across the Atlantic illustrate how environmental degradation and instability interact with existing social and economic vulnerabilities (International Organization for Migration 2023).

Narrative intelligence, defined as the systematic analysis of how stories, meanings, and interpretive frameworks shape human behavior and collective dynamics, offers a powerful lens for understanding these complex relationships (Mattern 2005; Bruner 2004; Miskimmon et al. 2013). Unlike approaches that seek to establish direct causal links between climate variables and security outcomes, narrative intelligence examines the intermediary processes through which environmental changes are interpreted, contested, and acted upon by diverse social actors (Burke et al. 2015; Scheffran et al. 2012). This approach recognizes that the pathway from climate stress to insecurity is mediated by the stories people tell about their experiences, the explanatory frameworks they adopt to make sense of their circumstances, and the collective identities that emerge from shared narratives of displacement and dispossession (Adger et al. 2014; Brown and Westaway 2011).

This amalgamation of climate, migration, and security narratives is particularly evident in contemporary European politics, where competing storylines about environmental displacement have reshaped both policy discourse and electoral dynamics (Lazaridis and Campani 2017; Hartmann 2010). European policymakers increasingly encounter climate migration through overlapping narratives of environmental crisis, cultural threat, and security vulnerability that blur traditional distinctions between humanitarian and defense-oriented responses (Bettini et al. 2017; Methmann and Oels 2015). Right-wing populist parties have proven especially adept at weaving climate migration into broader narratives of civilizational decline and national insecurity, portraying environmental displacement not as a collective problem requiring global cooperation but as evidence of impending social collapse that necessitates border fortification and cultural preservation (Veron 2010).

Progressive narratives, by contrast, frame climate migrants as victims of environmental injustice who deserve solidarity and protection. Yet these perspectives often struggle to gain traction in political environments dominated by securitized discourse. These competing narrative frameworks do not merely mirror policy preferences; they actively construct the political possibilities for European

responses to climate migration, determining whether environmental displacement is understood as a humanitarian challenge requiring assistance, a security threat demanding containment, or a justice issue calling for systemic transformation (Wunderlich 2012; Bourbeau 2015).

Case Study: Vulnerabilities in the Sahel

The relationship between climate change and migration in the Sahel has received extensive scholarly attention, with researchers documenting both the mechanisms and the patterns of climate-induced displacement. Eboreime et al. (2025) provide one of the most comprehensive analyses of this relationship in their study *From Drought to Displacement*. Their research demonstrates how prolonged drought conditions trigger multi-stage migration processes, beginning with short-term seasonal movements and escalating to permanent displacement when adaptive capacity is exceeded. The authors' epidemiological approach reveals that climate-induced migration in the Sahel follows predictable patterns related to rainfall variability and agricultural productivity. Their findings indicate that a ten percent decrease in seasonal rainfall correlates with a fifteen to twenty percent increase in migration flows from affected areas (Eboreime et al. 2025). This quantitative analysis provides critical evidence for understanding the scale and timing of climate-induced displacement across the region.

The Sahel's geographical position makes it uniquely vulnerable to climate change impacts. Van Ackern and Detges (2022) emphasize that its location between the Sahara Desert and the more humid savannas creates inherent climatic instability that is now exacerbated by global warming trends. Temperatures are rising one and a half times faster in the Sahel than in the rest of the world, and, according to the United Nations (2025), around eighty percent of agricultural land in the region is degraded, leaving approximately fifty million people who depend on livestock farming in competition for dwindling resources. Climate change in the Sahel manifests through increased drought frequency, erratic rainfall, and progressive desertification, producing what Van Ackern and Detges describe as a "cascade of vulnerabilities" that erodes multiple dimensions of human security. Sartori and Fattibene (2019) expand this framework by showing how environmental degradation operates as a "threat multiplier," amplifying socio-economic fragility and generating new security risks. Their analysis highlights how declining agricultural productivity, water scarcity, and ecosystem degradation interact with governance deficits to create conditions conducive to both migration and violent extremism.

As a result of global climate change, extreme weather events are becoming more frequent and severe. Long-term shifts in temperature and rainfall patterns are destabilizing entire communities, disrupting traditional livelihoods, and threatening food security (Bremberg 2019). Dieng (2021), writing in the International Review of the Red Cross, situates these developments within broader governance and development frameworks. Dieng argues that while climate change presents grave

challenges, it also offers opportunities for regional cooperation and sustainable development. However, realizing these opportunities requires addressing the structural vulnerabilities that make Sahelian societies so susceptible to climate shocks.

The European Institute of the Mediterranean (IEMed) estimates that up to thirteen million people in North Africa may be displaced by 2050, representing six percent of the population. In the Sahel and West Africa, projections suggest that as many as eighty-six million people could be forced to move within national borders by mid-century. Climate-related environmental stressors are already the leading cause of internal displacement worldwide, and climate change is increasingly recognized as a significant driver of human mobility in regions such as North Africa and the Sahel (Bassou 2019).

Recent data further reveals that more than ninety percent of displaced persons in Africa remain within their region of origin, primarily because of limited financial resources to support international migration. The Atlantic route from West Africa to Europe remains the most important pathway for those who do undertake migration to Europe. It became the most active irregular route from Africa to Europe in 2024, when 36,000 African migrants were intercepted. Overall, irregular African migration to Europe declined from 282,000 in 2023 to 146,000 in 2024, largely because of intensified European Union (EU)-funded interdiction efforts (Williams 2025). The Canary Islands experienced an eighteen percent increase in arrivals, reaching almost 27,730 in 2023, largely fueled by departures from Mauritania (Frontex 2023). Mali was the leading country of origin for irregular migration to Europe in 2024, with approximately 16,500 migrants, while Guinea topped the list in 2023 with about 21,700 individuals (Williams 2025).

Conversely, demographic pressures suggest that neighboring countries will not be able to absorb migration flows indefinitely. The Institute for Economics and Peace, a European think tank, currently estimates that 1.2 billion people are at risk of climate-related displacement worldwide by 2050 (Institute for Economics and Peace 2020). Migration in this context is often a last resort, pursued only after all other adaptation strategies fail. As conditions deteriorate, an increasing number of people are likely to look toward Europe as a potential lifeline (Yayboke and Aboneaaj 2025). Consequently, any further destabilization in the Sahel has direct repercussions for Europe, affecting not only its relationship with the African continent but also the cohesion among EU member states themselves.

1. Literature Review

The literature on the climate–migration–terrorism nexus employs a wide range of methodological approaches, from quantitative analyses of climate and conflict data to ethnographic studies of migration experiences. This methodological diversity

strengthens the overall evidence base while revealing critical gaps in current understanding. Several scholars emphasize the challenges of establishing clear causal relationships between climate change, migration, and terrorism. The complex and multi-causal nature of these phenomena makes it difficult to isolate the effects of climate variability from other structural factors such as governance, inequality, and socio-political exclusion. Most researchers, therefore, adopt a "contributory cause" framework rather than asserting direct causation. Despite routine claims linking Sahelian terrorism to environmental stress, current scientific evidence remains inconclusive regarding whether and how specific climatic factors influence conflict variability and terrorism (Sow and Kone 2024).

The literature also exposes substantial geographical and temporal gaps. While certain parts of the Sahel, such as northern Mali and Niger, have been studied extensively, others remain understudied. Moreover, much of the research focuses on developments since the 2010s, with limited historical analysis of longer-term climate–security dynamics. These gaps restrict the ability to identify enduring patterns or to assess how historical adaptation mechanisms might inform current responses.

The "threat multiplier" concept remains one of the most influential analytical frameworks in climate–security studies. It captures how climate change interacts with pre-existing political, social, and economic vulnerabilities to heighten security risks. The concept has been described as "definitional" for having established a baseline vocabulary for analyzing climate-related risks and shaping how security professionals conceptualize environmental threats (Goodman and Baudu 2023). Its influence within the United States national security institutions is particularly notable, as the framework has permeated defense planning and is widely adopted across the armed services. However, recent scholarship calls for moving beyond the "threat multiplier" framework, arguing that the phrase itself provides limited analytical precision. As one critique notes, "the language of threat multiplier does not tell you much about what combination of factors we should be worried about" (Busby 2020). If the concept merely implies that "bad things go together," its policy utility remains constrained. In response, newer frameworks seek to specify the mechanisms linking climate stress to security outcomes and to identify targeted interventions (Cullum 2024).

Other scholars employ "worldmaking" analysis to understand how the "threat multiplier" narrative shapes institutional practices. This body of work examines how conceptual framings of global risk translate into localized outcomes, showing that abstract security narratives have tangible effects on communities and governance (Cullum 2024). Such approaches underscore that the power of the "threat multiplier" framework lies not only in what it describes but in how it guides resource allocation, shapes political priorities, and structures international responses (Hassan and Mamshai 2023).

Meanwhile, empirical evidence linking climate change to terrorism in the Sahel remains contested. The consensus in the literature is that climate change does not directly increase terrorism in the Central Sahel. Instead, climate-induced disruptions to agricultural systems, resource scarcity, and local conflicts create the enabling conditions for violent extremism. These local conflicts provide fertile ground for terrorist groups to expand influence and recruit members (Institute for Security Studies 2024). Violent extremist groups, including factions associated with ISIS and al-Qaeda, increasingly embed themselves within communities already facing economic hardship and environmental decline. These organizations exploit competition over scarce water and arable land to attract those who feel marginalized or dispossessed, thereby deepening governance vacuums and accelerating social fragmentation. Mali and Burkina Faso now rank as the world's first and third most terrorism-affected countries (Tony Blair Institute for Global Change 2024). Larémont's (2021) research on climate change and conflict in the Western Sahel further supports this connection, demonstrating how extremist groups capitalize on climate-related grievances, using environmental narratives to justify violence and recruit supporters.

Efforts over the past decade to manage irregular migration through the Sahel have altered, but not halted, population movements. Migrants face greater risks as the illicit networks that facilitate their movement become more entrenched. Under European pressure, Niger adopted a 2015 law criminalizing migrant smuggling, leading to a sharp reduction in recorded flows through Agadez—from 330,000 in 2016 to 70,000 in 2017—an outcome celebrated by European policymakers (Center for Strategic and International Studies 2025). However, these securitization measures have constrained the application of the Economic Community of West African States (ECOWAS) Freedom of Movement protocols, limiting protection for individuals displaced by climate-related disasters (Morello and Rizk 2022).

The EU has also expanded counterterrorism and security cooperation across Africa. Yet, as Raineri's study *When (Fighting) Climate Change Fuels Terrorism* argues, top-down, uniform responses to environmental challenges often exacerbate tensions, creating what he terms "fertile ground for terrorist groups." The EU Council's 2024 conclusions similarly emphasize the need to strengthen collaboration with African-led counter-terrorism initiatives (United Nations 2022). The EU remains Africa's primary security partner, providing over ninety percent of the African Union's peace operations budget through the European Peace Facility, amounting to more than €2.25 billion (European Parliament 2020). The EU's contributions include three military training missions—Somalia (2010), Mali (2013), and the Central African Republic (2016)—as well as one naval operation (NAVFOR ATALANTA 2009) and three civilian capacity-building missions in Mali, Niger, and Somalia (European Parliament 2020).

Emerging literature also points to the growing influence of hybrid warfare and information manipulation in the Sahel. Russian "foreign information manipulation

and interference" (FIMI), a form of narrative warfare, has had a significant impact in sub-Saharan Africa (Terren, Van Aelst, and Van Damme 2025). FIMI serves as a key component of Russia's hybrid strategy, particularly in Burkina Faso and Mali (Duarte 2024; Benkler, Hansen, and Reichert 2022). Faleg (2022) further argues that Russian interference not only destabilizes local governance but also drives migration flows by amplifying insecurity and eroding state legitimacy.

The implications for Europe, while not yet comprehensively explored in the literature, are substantial. Climate-induced instability in the Sahel contributes to irregular migration pressures and generates ungoverned spaces that can serve as operational hubs for extremist groups. Continued displacement will increase migratory pressure along the Atlantic coast, the Canary Islands, and the Iberian Peninsula. The emerging scholarly consensus suggests that mitigating climate change in the Sahel is not only an environmental necessity but a cornerstone of both regional and international security strategy. As climate disruptions intensify, policymakers in Europe and beyond must address their security implications in vulnerable regions. The creation of international frameworks such as the Global Compact for Migration marks progress in recognizing climate displacement, yet implementation challenges and political resistance underscore the persistent difficulty of crafting effective multilateral responses to climate-driven migration and insecurity.

2. Research Methods and Results

This article uses a qualitative research methodology to draw on narrative intelligence from open-source intelligence (OSINT) geographically referenced to the Sahel. We reviewed news outlets and social media posts throughout the region to identify patterns of reporting related to migration associated with the countries in the Sahel and Europe. This search intends to capture current narratives relative to migration from the Sahel to Europe and combine those narratives with other contemporary literature to reflect the current narrative pertaining to the subject migratory flow.

The following analysis draws on narrative intelligence from open-source intelligence (OSINT) geographically referenced to the Sahel, where people and communities are experiencing significant climate-induced migration, examining how different narrative frameworks have shaped the trajectory from environmental stress to security outcomes (Brzoska and Fröhlich 2016; Abel et al. 2019). Through this lens, we demonstrate that effective counterterrorism and climate adaptation strategies must engage seriously with the power of stories to shape human behavior, moving beyond purely technical or military approaches to address the deeper narrative foundations of extremist appeal in the context of environmental change (Carius 2009; Detges 2016).

For the source categories, we conducted an open-source intelligence (OSINT). The data used in this analysis was collected through Seerist, a commercial geospatial

intelligence platform that aggregates and indexes global news media, social media, and open-source reporting in near real-time. Seerist's integrated search and geospatial referencing capabilities allowed the authors to systematically query content geographically bounded to the Sahel region and thematically filtered to the climate–migration–terrorism nexus. Boolean keyword searches were conducted using "Sahel" combined with "climate," "migration," or "Europe," joined by an AND operator against twelve country names: Senegal, Gambia, Mauritania, Guinea, Mali, Burkina Faso, Niger, Chad, Cameroon, Nigeria, Sudan, and South Sudan. Results were reviewed, then for relevance, and coded thematically in accordance with the narrative intelligence frameworks previously described. Scholarly journal results identified through Seerist were supplemented with grey literature, policy reports, and multilateral assessments relevant to the subject matter.

The reporting indicates that African migrants have become pawns in European countries' domestic political struggles, as center-right parties attempt to appease growing anti-migrant sentiment by adopting the rhetoric and policies of national-conservative and even far-right parties. Six EU member states currently have far-right leaders at their helm: Italy, Finland, Hungary, Slovakia, Croatia, and the Czech Republic (Zarhloule 2025). National, xenophobic rhetoric is no longer contained to the fringes of the political spectrum across the EU, with anti-immigrant sentiment today featuring dominantly in public debates after years of far-right populists amplifying cultural anxieties and accusing governments of having lost control of their sovereign borders (Varma and Roehse 2024).

The Narrative Intelligence Lens

Applying the analytical tool of narrative intelligence to the climate-migration-terrorism nexus reveals how deeply embedded story frameworks shape security thinking and policy responses within the EU. Narrative intelligence, understood as the systematic analysis of stories, symbols, and meaning-making processes, exposes the emotional and cognitive underpinnings of institutional behavior and strategic decision-making. For instance, the EU's approach to migration policy demonstrates how competing story frameworks generate divergent and often conflicting policy outcomes. Table 1 below gives the main narratives in the literature regarding the climate-migration-terrorism nexus as it applies to the Sahel and the EU.

Table no. 1 represents the qualitative narrative intelligence analysis to examine how the climate–migration–terrorism nexus in the Sahel is framed in the academic and policy literature. Rather than testing causal claims, the objective is to identify recurring narrative patterns, dominant frames, and associated policy prescriptions. This analysis proceeded in three stages. First, the literature used for this report was organized around three analytically distinct but overlapping domains: (1) climate security, (2) migration, and (3) terrorism/political violence in the Sahel. The sources included peer-reviewed scholarship, policy reports, government documents, news articles, and multilateral assessments.

TABLE no. 1. Narrative Themes

Theme/ Nexus	Narrative	Framing/Storyline	Policy Implications
Migration	Fortress Europe	Migration as a threat to social cohesion, sovereignty, and border	Externalization of border control, hotspots, partnerships with origin/transit states, and restrictive policies
	Humanitarian / Solidarity	Migration as a moral and legal obligation, tied to human rights and European values	Emphasis on protection, integration, and international responsibility; tensions within EU institutions
	Adaptation	Migration as a natural response to environmental and social change	Policies favoring accommodation, flexible management strategies
	Contribution	Migrants as social and economic assets	Integration, capacity-building, leveraging migrants' potential
	Protection	Focus on migrants' rights and vulnerabilities	Humanitarian protection, addressing broader regional stability linked to migrant insecurity
Climate Security	Threat Multiplier	Climate change accelerates existing instability (conflict, displacement, state fragility)	Security policies framed in crisis and risk management terms
	Systemic Risk	Climate-induced cascading failures across food, energy, and financial systems	Risk assessment, resilience planning across interconnected systems
	Transformation	Climate change as an opportunity for adaptation, cooperation, and resilience	Emphasis on innovation, resilience-building, and cooperative security strategies
Terrorism/ Extremism	Grievance-Based / Identity	Exploits collective grievances, injustice, and identity crises	Recruitment, radicalization, and legitimization of violence
	Counterterrorism Narrative	State responses shape legitimacy; they can reinforce or undermine trust	Policies may unintentionally fuel narratives of exclusion or injustice
	Digital Contest	Competing narratives on social media shape identity and political agency	Need for narrative-aware communication strategies; monitoring online radicalization

Theme/ Nexus	Narrative	Framing/Storyline	Policy Implications
Intersecting Nexus: Climate – Migration Terrorism	Climate Refugee	Links environmental degradation to displacement and security risk	Securitized migration policies; may oversimplify complex migration dynamics
	Migration–Terrorism	Links migration with radicalization, foreign fighters, porous borders	Justifies preventive, exclusionary policies; can misrepresent empirical realities
	Convergent Narratives (Fortress + Climate Refugee)	Amplifies crisis logic	Promotes containment, exclusion, potentially increasing instability
	Integrative Narratives (Adaptation + Transformation + Contribution)	Emphasizes resilience, cooperation, and human security	Supports holistic, sustainable, human-centric policy responses

Second, an inductive thematic coding process was applied. Texts were read systematically to identify recurring claims, metaphors, causal linkages, and descriptive patterns. These narratives were coded based on repetition and salience across sources, allowing dominant storylines to emerge (e.g., climate as a "threat multiplier," migration as a security risk, environmental scarcity as a driver of radicalization).

Third, a framing analysis was conducted to assess how these narratives structured problem definition, attribution of responsibility, and proposed policy responses. Particular attention was paid to whether climate variability was framed as a direct driver of terrorism, an indirect stressor mediated by governance failures, or part of broader socio-political fragility. Policy implications embedded within each narrative were catalogued and compared.

This approach does not attempt statistical generalization, nor should it be used to determine causal inference. Rather, it provides a structured baseline mapping of dominant interpretive frameworks shaping discourse on the Sahelian nexus. By clarifying how problems are constructed in the literature, the analysis contributes to understanding how certain policy pathways become privileged while others are marginalized. Since the 2015 migration crisis, the dominant European narrative has oscillated between humanitarian obligation and existential threat (Geddes and Scholten 2016). The "fortress Europe" narrative, which frames migration as a danger to social cohesion, sovereignty, and border integrity, has legitimized the externalization of border controls, the establishment of hotspots, and partnerships with origin and transit states designed to halt migration before it reaches European territory (Lazaridis and Wadia 2015; Carrera et al. 2019).

Alternative narratives rooted in European values of solidarity, human rights, and international responsibility have created persistent tensions within EU institutions and among member states. This contestation helps explain the repeated failure of comprehensive migration reform, as different actors operate from incompatible story frameworks regarding what migration means for European identity and security (Triandafyllidou 2018). Understanding these competing narratives reveals why technical and administrative solutions repeatedly founder on political disagreements grounded in deeper symbolic interpretations of Europe's borders and moral responsibilities (Hampshire 2013).

Beyond the "invasion" or "crisis" narrative that justifies defensive measures and exclusionary practices (Bigo 2002), alternative storylines open space for more constructive policy approaches. The "adaptation" narrative views migration as a natural human response to environmental and social change, promoting management strategies focused on accommodation rather than prevention (Tacoli 2009). The "contribution" narrative highlights migrants as social and economic assets, pointing toward integration and capacity-building approaches (Castles 2004). The "protection" narrative centers on the rights and vulnerabilities of migrants themselves, emphasizing that insecurity among mobile populations can translate into broader regional instability (Lyons 2025).

Meanwhile, the climate-related security discourse also operates through multiple and competing narrative frameworks. The "threat multiplier" narrative positions climate change as an accelerant of existing instability, where drought intensifies resource conflicts, sea-level rise displaces populations, and extreme weather events overwhelm state capacity (CNA Corporation 2007). This framing allows security institutions to conceptualize climate change through familiar paradigms of risk, conflict, and crisis. Other narratives, however, reveal alternative pathways of understanding. The "systemic risk" narrative emphasizes cascading failures across interconnected systems such as food production, energy infrastructure, and financial markets (O'Brien et al. 2018). The "transformation" narrative reframes climate change as an opportunity for resilience-building and cooperative security, focusing on adaptation and innovation as sources of stability (Nelson, Adger, and Brown 2007). Each framework highlights certain dynamics while obscuring others, illustrating that climate security is not an objective condition but a narrative construct that reflects underlying assumptions about agency, causality, and responsibility.

Narrative intelligence further clarifies how extremist organizations construct and weaponize stories to mobilize support. Terrorist narratives draw upon collective grievances, identity crises, and perceptions of injustice to legitimize violence and provide adherents with a sense of moral purpose (Hoffman 2006). Counterterrorism policies, in turn, generate their own narratives that can either reinforce or undermine state legitimacy. In the digital age, social media has intensified this narrative contest, creating dynamic spaces where terrorist organizations, states, civil society actors,

and ordinary citizens compete to define identity, belonging, and political agency (Conway 2017).

At the intersection of climate, migration, and terrorism, overlapping storylines produce a self-reinforcing logic of crisis. The narrative of the "climate refugee" links environmental degradation to mass displacement and security risk (Myers 2002). While this story has helped raise awareness of the connections between environmental stress and human mobility, it often simplifies complex migration decisions and promotes securitized policy responses (Bettini, Nash, and Whitfield 2013). Similarly, narratives that link migration and terrorism, whether through tropes of radicalized diasporas, foreign fighters, or porous borders, create causal associations that lack empirical grounding but shape policy discourse and public opinion (Ibrahim 2005).

The narrative reporting further reveals that European governments acknowledge climate change and terrorism as drivers of African migration, yet respond primarily with containment, externalization, and anti-immigrant politics rather than addressing root causes. The EU's strategy of outsourcing border control to often-authoritarian African governments has been widely criticized for human rights abuses, lack of accountability, and failure to provide sustainable solutions, while failing to address the fundamental drivers of migration, including climate change, conflict, and economic inequality. This is particularly acute along the Atlantic route, which is a longer voyage to Europe, fraught with danger. These intersecting narratives matter because they reinforce one another across institutional and societal domains, shaping the policy imagination of what constitutes a security problem and what responses appear legitimate. For example, when the "fortress Europe" and "climate refugee" narratives converge, they justify preventive and exclusionary approaches that may inadvertently increase regional instability and human insecurity. Conversely, integrating "adaptation," "transformation," and "contribution" narratives could enable more holistic responses grounded in resilience, cooperation, and human security.

3. Implications for Practitioners

The traditional security paradigm, focused on military threats and state-to-state conflicts, struggles to adequately address the complex, interconnected challenges of the 21st century. Climate change, migration, and terrorism represent security threats that transcend borders, evolve rapidly, and resist conventional analytical frameworks. Narrative intelligence encompasses the ability to recognize, analyze, and strategically employ the stories that drive human behavior and institutional responses. Unlike traditional intelligence that focuses primarily on facts and data, narrative intelligence examines how information is packaged, transmitted, and interpreted through story structures that give meaning to events and shape responses to them (Mattern 2005). This approach recognizes that security challenges are not merely

objective phenomena but are fundamentally shaped by how they are understood, communicated, and acted upon by various stakeholders. The stories we tell about climate change, migration, and terrorism directly influence policy responses, public support, and the effectiveness of security measures (Jackson 2005).

Implementing narrative intelligence in security analysis requires systematic attention to story structures, narrative actors, and the strategic dimensions of storytelling. Security analysts can develop narrative mapping techniques that identify dominant stories about challenges, trace their sources and transmission pathways, and assess their influence on different audiences (Antoniades, Miskimmon, and O'Loughlin 2010). This approach involves analyzing not just what stories are being told, but who is telling them, through what channels, to which audiences, and with what effects. It requires understanding how narratives compete, combine, and evolve over time, and how they interact with events, policies, and other narratives (Miskimmon, O'Loughlin, and Roselle 2013).

Narrative intelligence also suggests the importance of reflexivity in security analysis, recognizing how analysts' own narrative frameworks shape their understanding of security challenges. The stories that security institutions tell about themselves, their missions, and their methods influence their capacity to understand and respond to complex challenges (Weldes et al. 1999). Beyond analysis, narrative intelligence offers tools for strategic engagement with security challenges. This involves developing communication strategies that work with rather than against dominant narrative currents, finding ways to connect security objectives with stories that resonate with key audiences. For climate security, this might mean connecting climate action with narratives of resilience, innovation, and economic opportunity rather than relying solely on threat-based framings (O'Neill and Nicholson-Cole 2009). For migration, it could involve developing stories that acknowledge legitimate concerns about change while highlighting successful integration and mutual benefit (Zapata-Barrero et al. 2017). For counterterrorism, it might mean crafting counter-narratives that address underlying grievances while delegitimizing violent methods (Braddock and Horgan 2016).

Conclusion

The EU remains committed to supporting refugees, displaced populations, and host communities, while continuing to collaborate with international partners to address the root causes of irregular migration and forced displacement. It also seeks to strengthen governance and management capacities in partner countries to ensure more sustainable and humane migration outcomes (European External Action Service 2025). The interconnected dynamics of climate change, migration, and terrorism in the Sahel present one of the most pressing and complex security challenges of the 21st century. Though the causal relationships among these variables remain deeply context-dependent, the evidence consistently indicates that climate

change functions as a "threat multiplier," intensifying existing vulnerabilities and creating new layers of insecurity across environmental, social, and political domains.

Traditional security frameworks, focused narrowly on capabilities, intentions, and material conditions, are insufficient to capture the full complexity of these challenges. The interrelationship between climate change, migration, and terrorism is deeply embedded in the stories that societies tell about causation, responsibility, and response. Understanding these phenomena, therefore, requires engaging with the narratives that shape perception and drive action.

Narrative intelligence also provides a vital analytical framework for this task. It illuminates how meaning-making processes construct security challenges and influence policy responses. By examining how narratives circulate, evolve, and compete, this approach enables policymakers to identify both opportunities for cooperation and potential sources of conflict. Applying narrative intelligence to the climate–migration–terrorism nexus thus requires new analytical competencies, institutional adaptation, and strategic foresight. It calls for sensitivity to temporal dynamics, awareness of competing narrative frames, and reflexivity in how security itself is conceptualized. Most importantly, narrative intelligence reminds us that stories are not peripheral to policy, they are central to how human societies interpret and manage crises. Recognizing this opens the possibility of crafting more resonant, legitimate, and effective responses to global security challenges. In an era defined by accelerating environmental change and transnational instability, the strategic use of narrative intelligence may become indispensable to effective security governance.

Future research should deepen understanding of the causal mechanisms linking climate change to migration and terrorism while expanding comparative and longitudinal analyses across regions. Policy responses must integrate environmental, social, and security dimensions, emphasizing coordination between European, African, and multilateral institutions. Addressing the security implications of climate change in the Sahel is therefore not only an environmental necessity but a strategic imperative for global stability and shared human security.

Funding Statement
The authors did not receive any funding in connection with the preparation of this manuscript.
Conflict of Interest Disclosure:
The authors declare that they do not have any financial, personal, or professional relationships that could inappropriately influence their research.

References

Abel, G.J., M. Brottrager, J. Crespo Cuaresma and R. Muttarak. 2019. "Climate, conflict and forced migration." Global Environmental Change 54*:* 239–249. https://doi.org/10.1016/j.gloenvcha.2018.12.003.

Adger, W. N., et al. 2014. *Human security.* In Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change, edited by C. B. Field, V. R. Barros, D. J. Dokken, K. J. Mach, M. D. Mastrandrea, T. E. Bilir, M. Chatterjee, K. L. Ebi, Y. O. Estrada, R. C. Genova, B. Girma, E. S. Kissel, A. N. Levy, S. MacCracken, P. R. Mastrandrea, and L. L. White, 755–791. Cambridge University Press.

Antoniades, A., A. Miskimmon, and B. O'Loughlin. 2010. "Great power politics and strategic narratives." The Centre for Global Political Economy Working Paper 7*:* 1–32.

Bassou, A., A. Chmielewska, and X. Ruiz-Campillo. 2019. Climate security in the Sahel and the Mediterranean: Local and regional responses. https://www.iemed.org/publication/climate-security-in-the-sahel-and-the-mediterranean-local-and-regional-responses/.

Benkler, M., A.S. Hansen, and L. Reichert. 2022. Protecting the truth: Peace operations and disinformation. Center for International Peace Operations. https://reliefweb.int/report/world/protecting-truth-peace-operations-and-disinformation.

Bettini, G. 2013. "Climate barbarians at the gate? A critique of apocalyptic narratives on 'climate refugees'." Geoforum 45*:* 63–72. https://doi.org/10.1016/j.geoforum.2012.09.009.

Bettini, G., S.L. Nash, and G. Whitfield. 2017. *Relational climate politics: The European Union and the climate-migration nexus*. In Climate Diplomacy (pp. 219–235). Springer.

Bigo, D. 2002. "Security and immigration: Toward a critique of the governmentality of unease." Alternatives 27(1): 63–92. https://migrantsproject.eu/wp-content/uploads/2020/08/Bigo_Security-and-Immigration.pdf.

Boas, I. 2015. *Climate migration and security: Securitisation as a strategy in climate change politics*. Routledge.

Bourbeau, P. 2015. "Migration, resilience and security: Responses to new inflows of asylum seekers and migrants." Journal of Ethnic and Migration Studies 41(12): 1958–1977. https://doi.org/10.1080/1369183X.2015.1047331.

Bremberg, N. 2019. *The European Union and Climate-Related Risks: A Case Study of the Sahel.* in *Climate Security in the Sahel and the Mediterranean: Local and Regional Responses.* Ed. A. Bassou, et al. EuroMesco Joint Policy Study 13. https://www.iemed.org/wp-content/uploads/2021/01/Joint-Policy-Study_13_Climate-Security-in-the-Sahel-and-the-Mediterranean.pdf.

Brown, K., and E. Westaway. 2011. "Agency, capacity, and resilience to environmental change: Lessons from human development, well-being, and disasters." Annual Review of Environment and Resources 36*:* 321–342. https://doi.org/10.1146/annurev-environ-052610-092905.

Bruner, J. 2004. "Life as narrative." Social Research 71(3): 691–710. https://www.jstor.org/stable/40970444.

Brzoska, M., and C. Fröhlich. 2016. "Climate change, migration and violent conflict: Vulnerabilities, pathways and adaptation strategies." Migration and Development 5(2): 190–210. https://doi.org/10.1080/21632324.2015.1022973.

Buhaug, H. 2015. "Climate–conflict research: Some reflections on the way forward." WIREs Climate Change 6(3): 269–275. https://doi.org/10.1002/wcc.336.

Burke, M., S.M. Hsiang, and E. Miguel. 2015. "Global non-linear effect of temperature on economic production." Nature 527(7577): 235–239. https://doi.org/10.1038/nature15725.

Busby, J. 2020. "It's time we think beyond 'threat multiplier' to address climate and security. New Security Beat". https://www.newsecuritybeat.org/2020/01/its-time-threat-multiplier-address-climate-security/.

Carius, A. 2009. *Climate change and security in Africa: Challenges and international policy context.* In Climate change and security in Africa (pp. 25–44). Nordic Africa Institute.

Carrera, S., N.C. Luk, J. Allsopp, and L. Vosyliūtė. 2019. *The external dimensions of EU migration and asylum policies in times of crisis*. In Constructing and negotiating migration and asylum in Europe (pp. 58–84). Springer.

Castles, S. 2004. "Why migration policies fail." Ethnic and Racial Studies 27(2): 205–227. https://doi.org/10.1080/0141987042000177306.

Center for Climate and Security. 2023. Climate change as a "threat multiplier": History, uses and future of the concept. https://climateandsecurity.org/2023/01/briefer-climate-change-as-a-threat-multiplier-history-uses-and-future-of-the-concept/.

CNA Corporation. 2007. National security and the threat of climate change. CNA Corporation. https://www.cna.org/archive/CNA_Files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf.

Conway, M. 2017. "Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research." Studies in Conflict and Terrorism 40(1): 77–98. https://doi.org/10.1080/1057610X.2016.1157408.

Cullum, R. 2024. "Making a world of climate insecurity: The threat multiplier frame and the US national security community." Global Studies Quarterly 4(4): ksae085. https://doi.org/10.1093/isagsq/ksae085.

Detges, A. 2016. "Local conditions of drought-related violence in sub-Saharan Africa: The role of road and water infrastructures." Journal of Peace Research 53(5): 696–710. https://doi.org/10.1177/0022343316651922.

Dieng, A. 2021. "The Sahel: Challenges and opportunities." International Review of the Red Cross 103(918): 765–779. https://doi.org/10.1017/S1816383122000339.

Duarte, F.P. 2024. "Information disorder and civil unrest: Russian weaponization of social media platforms in Mali and Burkina Faso – 2020–2022." African Security 17(3–4): 205–223. https://doi.org/10.1080/19392206.2024.2423139.

Eboreime, E., O. Anjorin, C. Obi-Jeff, T.M. Ojo, and A. Hertelendy. 2025. "From drought to displacement: Assessing the impacts of climate change on conflict and forced migration in West Africa's Sahel region." The Journal of Climate Change and Health 23*:* 100448. https://doi.org/10.1016/j.joclim.2025.100448.

Entman, R.M. 1993. "Framing: Toward clarification of a fractured paradigm." *Journal of Communication* 43(4): 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x.

European External Action Service. 2025. Migration and forced displacement. https://www.eeas.europa.eu/eeas/migration-forced-displacement_en.

European Parliament. 2020. Report on EU-African security cooperation in the Sahel region, West Africa and the Horn of Africa (2020/2002(INI))). https://www.europarl.europa.eu/doceo/document/A-9-2020-0129_EN.html.

___. 2021. Parliamentary question on climate change mitigation policies creating a breeding ground for terrorism (E-004838/2021). https://www.europarl.europa.eu/doceo/document/E-9-2021-004838_EN.html.

Farbotko, C., and C. McMichael. 2019. "Voluntary immobility: Indigenous voices in the Pacific." Forced Migration Review 61*:* 81–83. https://ora.ox.ac.uk/objects/uuid:d58a23e1-4873-46f2-a787-79c6c967b0b8/files/sxk81jm63x.

Frontex. 2023. "Record arrivals on Western African route in October." https://www.frontex.europa.eu/media-centre/news/news-release/record-arrivals-on-western-african-route-in-october-uNCHfO.

Geddes, A., and P. Scholten. 2016. The politics of migration and immigration in Europe (2nd ed.). SAGE Publications.

Gemenne, F., J. Barnett, W.N. Adger, and G.D. Dabelko. 2014. "Climate and security: Evidence, emerging risks, and a new agenda." Climatic Change 123*(*1): 1–9. https://doi.org/10.1007/s10584-014-1074-7.

Goffman, E. 1974. *Frame analysis: An essay on the organization of experience.* Harvard University Press.

Goodman, S., and P. Baudu. 2023. "Climate Change as a 'Threat Multiplier': History, Uses and Future of the Concept." Briefer No. 38. Center for Climate and Security / Council on Strategic Risks.

Hampshire, J. 2013. The politics of immigration: Contradictions of the liberal state. Polity Press.

Hartmann, B. 2010. "Rethinking climate refugees and climate conflict: Rhetoric, reality and the politics of policy discourse." Journal of International Development 22(2): 233–246. https://doi.org/10.1002/jid.1676.

Hassan, F. and A. Mamshai. 2023. "Climate change as a threat multiplier": Security and communal implications for Iraq. Community Change 4(2). https://doi.org/10.21061/cc.v4i2.a.41.

Hoffman, B. 2006. Inside terrorism (Rev. ed.). Columbia University Press.

Hunter, L.M., J.K. Luna, and R.M. Norton. 2015. "Environmental dimensions of migration." Annual Review of Sociology 41: 377–397. https://doi.org/10.1146/annurev-soc-073014-112223.

Ibrahim, M. 2005. "The securitization of migration: A racial discourse." International Migration 43(5): 163–187. https://onlinelibrary.wiley.com/doi/10.1111/j.1468-2435.2005.00345.x.

Ide, T. 2018. "Climate war in the Middle East? Drought, the Syrian civil war and the state of climate–conflict research." Current Climate Change Reports 4(4): 347–354. https://doi.org/10.1007/s40641-018-0115-0.

Institute for Economics and Peace 2020. *Ecological Threat Register 2020 : Understanding Ecological Threats, Resilience, and Peace.* https://www.economicsandpeace.org/wp-content/uploads/2023/10/ETR-2020-web.pdf.

Jackson, R. 2005. Writing the war on terrorism: Language, politics and counter-terrorism. Manchester University Press.

Koubi, V., G. Spilker, T. Böhmelt, and T. Bernauer. 2018. "Do natural resources matter for interstate and intrastate armed conflict?" Journal of Peace Research 51(2): 227–243. https://doi.org/10.1177/0022343313493455.

Larémont, R.R. 2021. "Climate change and conflict in the Western Sahel." African Studies Review 64(4): 748–759. https://doi.org/10.1017/asr.2021.114.

Lazaridis, G., and G. Campani, eds. 2017. Understanding the populist shift: Othering in a Europe in crisis. Routledge.

Lazaridis, G., and K. Wadia, eds. 2015. The securitisation of migration in the EU: Debates since 9/11. Palgrave Macmillan.

Lyons, W. 2025. Climate Change, Migration, and Terrorism in the Sahel: A Narrative Intelligence Approach to European and Atlantic Security Challenges. *Climate Change and Security Challenges in the Atlantic*, 39.

Mattern, J.B. 2005. Ordering international politics: Identity, crisis, and representational force. Routledge.

McMichael, C., J. Barnett, and A.J. McMichael. 2012. "An ill wind? Climate change, migration, and health." Environmental Health Perspectives 120(5): 646–654. https://doi.org/10.1289/ehp.1104375.

Methmann, C., and A. Oels. 2015. "From 'fearing' to 'empowering' climate refugees: Governing climate-induced migration in the name of resilience." Security Dialogue 46(1): 51–68. https://doi.org/10.1177/0967010614552548.

Miskimmon, A., B. O'Loughlin, and L. Roselle. 2013. Strategic narratives: Communication power and the new world order. Routledge.

Morello, G. and J. Rizk. 2022. "Conflict, climate change and the shrinking mobility space in the Central Sahel." *Forced Migration Review* 69. https://www.fmreview.org/climate-crisis/morello-rizk/.

Mortreux, C., and J. Barnett. 2017. "Adaptive capacity: Exploring the research frontier." Wiley Interdisciplinary Reviews: Climate Change 8(4): e467. https://doi.org/10.1002/wcc.467.

Myers, N. 2002. "Environmental refugees: A growing phenomenon of the 21st century." Philosophical Transactions of the Royal Society B 357(1420): 609–613. doi: 10.1098/rstb.2001.0953.

Nelson, D.R., W.N. Adger, and K. Brown. 2007. "Adaptation to environmental change: Contributions of a resilience framework." Annual Review of Environment and Resources 32: 395–419. https://doi.org/10.1146/annurev.energy.32.051807.090348.

O'Brien, K., and J. Barnett. 2013. "Global environmental change and human security." Annual Review of Environment and Resources 38: 373–400. https://www.annualreviews.org/content/journals/10.1146/annurev-environ-032112-100655.

O'Brien, K., B. Kristoffersen, S. Self, B. Hayward, J. Maxwell, and L. Sygna. 2018. "Climate change as a threat multiplier for human disaster and conflict." Peace Research Institute Oslo.

Office of the High Commissioner for Human Rights. 2018. Global Compact for Safe, Orderly and Regular Migration (GCM). https://www.ohchr.org/en/migration/global-compact-safe-orderly-and-regular-migration-gcm.

Pelling, M., and C. High. 2013. "Understanding adaptation: What can social capital offer assessments of adaptive capacity?" Global Environmental Change 23(1): 308–318. https://doi.org/10.1016/j.gloenvcha.2005.02.001.

Raineri, L. 2020. "Sahel climate conflicts? When (fighting) climate change fuels terrorism." EUISS Conflict Series. https://www.iss.europa.eu/publications/briefs/sahel-climate-conflicts-when-fighting-climate-change-fuels-terrorism.

Reyer, C.P., et al. 2017. "Climate change impacts in Latin America and the Caribbean and their implications for development." Regional Environmental Change 17(6): 1601–1621. https://doi.org/10.1007/s10113-015-0854-6.

Rüttinger, L., D. Smith, G. Stang, D. Tänzler, and J. Vivekananda. 2015. A new climate for peace: Taking action on climate and fragility risks. Adelphi.

Sartori, N., and D. Fattibene. 2019. *Human security and climate change: Vulnerabilities in the Sahel.* EuroMesco Policy Brief No. 94. https://www.euromesco.net/wp-content/uploads/2019/02/Brief94_Human-Security-and-Climate-Change_Vulnerabilities-in-the-Sahel.pdf.

Scheffran, J., M. Brzoska, J. Kominek, P.M. Link, and J. Schilling. 2012. "Climate change and violent conflict." Science 336(6083): 869–871. https://doi.org/10.1126/science.1221339.

Schleussner, C.F., J.F. Donges, R.V. Donner, and H.J. Schellnhuber. 2016. "Armed-conflict risks enhanced by climate-related disasters in ethnically fractionalized countries." Proceedings of the National Academy of Sciences 113(33): 9216–9221. https://doi.org/10.1073/pnas.1601611113.

Sow, D. and F. Kone. 2024. "Does climate change fuel terrorism in the Sahel? Institute for Security Studies." https://issafrica.org/iss-today/does-climate-change-fuel-terrorism-in-the-sahel.

Tacoli, C. 2009. "Crisis or adaptation? Migration and climate change in a context of high mobility." Environment and Urbanization 21(2): 513–525. https://journals.sagepub.com/doi/10.1177/0956247809342182.

Terren, L., P. Van Aelst, and T. Van Damme. 2025. "The last line of defence: Measuring resilience to foreign information manipulation and interference in West Africa. European Union Institute for Security Studies." https://www.iss.europa.eu/publications/briefs/last-line-defence-measuring-resilience-foreign-information-manipulation-and.

Tony Blair Institute for Global Change. 2024. "From crisis to conflict: Climate change and violent extremism in the Sahel." https://institute.global/insights/geopolitics-and-security/from-crisis-to-conflict-climate-change-and-violent-extremism-in-the-sahel.

Torelli, S. 2020. Climate-driven migration in Africa. European Council for Foreign Relations. https://ecfr.eu/article/commentary_climate_driven_migration_in_africa/.

Torres, J. M., and Casey, J. A. 2017. "The centrality of social ties to climate migration and mental health." BMC Public Health 17(1): 600. https://doi.org/10.1186/s12889-017-4508-0.

Triandafyllidou, A. 2018. Handbook of migration and globalisation. Edward Elgar Publishing.

United Nations. 2022. "Countering terrorism in Africa requires preventive approach including respect for human rights, law." https://press.un.org/en/2022/sc15102.doc.htm.

___. 2025. "Efforts to address root causes of conflict, mitigate impact of climate change in West Africa, Sahel must be supported." https://press.un.org/en/2025/sc16036.doc.htm.

Van Ackern, P., and A. Detges. 2022. *Climate change, vulnerability and security in the Sahel. Three scenarios for Burkina Faso, Mali, and Niger in 2050.* CASCADES Report. https://www.cascades.eu/wp-content/uploads/2023/01/CASCADES_Scenarios_Sahel_final-EN-with-back-cover.pdf.

Varma, T., and S. Roehse. 2024. Understanding Europe's turn on migration. Brookings Institution Press.

Veron, P. 2010. *Occidentalism as counter-hegemonic discourse: The case of post-apartheid South Africa*. In Occidentalisms in the Arab world (pp. 165–187). I.B. Tauris.

Weldes, J., M. Laffey, H. Gusterson, and R. Duvall, eds. 1999. Cultures of insecurity: States, communities, and the production of danger. University of Minnesota Press.

Williams, W. 2025. African migration trends to watch in 2025. Africa Center for Strategic Studies. https://africacenter.org/spotlight/migration-trends-2025/.

Wilson Center. 2024. "Threat multiplier: Climate change and national security." https://www.wilsoncenter.org/video/threat-multiplier-climate-change-and-national-security.

Wunderlich, D. 2011. "Europeanization through the grapevine: Communication gaps and the role of international organizations in implementation networks of EU external migration policy." Journal of European Integration 34(5): 485–503. https://doi.org/10.1080/07036337.2011.611385.

Yayboke, E. and R. Aboneaaj. 2025. Peril in the desert: Irregular migration through the Sahel. Center for Strategic and International Studies. https://www.csis.org/analysis/peril-desert-irregular-migration-through-sahel.

Zarhloule, Y. 2025. Migrants at the gate: Europe tries to curb undocumented migration. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Zarhloule_EU.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

FIMI and Collective Security: The Role of Information Manipulation on Contemporary International Relations

Daniel-Horea BOGDAN*

*MA in security studies, Babes-Bolyai University, Faculty of History and Philosophy, Cluj-Napoca, Romania
e-mail: bogdan.danielh@yahoo.com

Abstract

This article evaluates the strategic reconfiguration of the European Union, marking the transition from conventional methods of combating disinformation to the implementation of the paradigm of Foreign Information Manipulation and Interference (FIMI). In the current security architecture, this concept becomes the central pillar in the process of securitization of the European information space. The article starts from the assumption that the geopolitical dynamics of 2026 are defined by volatility, and the conclusions of the report of the European External Action Service (EEAS) on the multiplication of hybrid state-origin aggressions validate this hypothesis. Attention is concentrated on Romania's structural vulnerabilities, as state actors can exacerbate internal crises to fragment societal cohesion and induce political instability. The study shows that, in the specific context of the eastern flank, defensive architecture can no longer be limited to an exclusively military or technological response. The results highlight the need for citizen-level cognitive resilience, making media literacy a vital component of national security. It is also necessary to adopt the „whole-of-society" model, supported by inter-institutional cooperation, which guarantees the integrity of democratic processes in the face of an information war in permanent development.

Keywords:
Insecurity; Risks; Threats; Vulnerabilities; Hybrid Warfare; Manipulation; Cognitive Resilience.

Article info
Received: 13 February 2025; Revised: 25 February 2025; Accepted: 18 March 2025; Available online: 8 April 2026

Citation: Bogdan, D.H. 2026. "FIMI and Collective Security: The Role of Information Manipulation on Contemporary International Relations." *Bulletin of "Carol I" National Defence University*, 15(1): 29-38. https://doi.org/10.53477/2284-9378-26-02

Preliminary considerations

In the contemporary strategic context, controlling the information field is no longer just an extension of public diplomacy, as it has become a critical component of national security and the strategic sector. The current relevance of the theme is imposed by unpredictable developments in the security environment, where hostile actors have modernized their modes of operation. The scientific novelty of this paper lies in the application of the new FIMI Exposure Framework, introduced in March 2025, on the specific vulnerabilities of the information space in Romania. The central objective is to examine how the EU, through the EEAS, has redefined the fight against disinformation under the integrated concept of FIMI, as well as the way in which aggressor countries adapt their techniques to pass under the radar of responsible institutions, with the main purpose of eroding citizens' trust in national defense and security institutions.

The research question of the paper is the following: to what extent does the adoption of the FIMI structure support the transition to a proactive position in securing the Romanian information space? Methodologically, the study uses a qualitative analysis of strategic documents published by NATO and the EEAS (2022-2025 period) to identify those mechanisms that contribute to reconfiguring national resilience. Thus, the research explains how this theoretical concept is translated into practical mechanisms that strengthen the resilience of the state in the face of external interference. This research method allows identifying the mechanisms by which information is transformed into a weapon by hostile actors, facilitating the securitization of digital space through rigorous attribution methods. The impact assessment is carried out through three operational indicators: the complexity of the technical infrastructure, the mapping of tactics through DISARM (Disinformation Analysis and Risk Management), and the analysis of the impact on the cognitive resilience of the Romanian population.

The practical importance of the study lies in the ability to identify the most important strategic assumptions related to the fight against FIMI that Romania can use as a collective response, together with the organizations it is part of, namely the EU and NATO. From a methodological point of view, the research expands by analyzing statistical data related to the impact of hybrid threats on national stability, providing an applied perspective on how Russian proxies act on the eastern flank. The analysis investigates the mechanisms of content localization and the use of artificial intelligence for the penetration of narratives in the Romanian cognitive space, identifying the vulnerabilities that state actors turn into security vulnerabilities.

The shift from reactive content analysis to proactive identification of handling infrastructures under the DISARM framework is the foundation of a new security culture. The evolution of this new paradigm depends fundamentally on how effectively the "whole-of-society" concept is implemented, which extends protection

beyond the technical barriers of infrastructure to the information security of the population. The research aims to provide answers that could be included in sustainable resilience strategies, and the approach supports efforts to strengthen the security of the digital ecosystem in Romania, adapting it to current challenges.

Conceptual clarifications

To substantiate the study, it is necessary to delimit the concept of securitization, defined as the act by which a problem is transformed from an ordinary political matter into an existential threat to a related object (Stritzel 2014). In the Strategic Compass 2022 vision, the information space is seen as an area of struggle where the EU must assume a proactive defensive posture (European Council 2022).

Hybrid warfare is a type of conflict that uses conventional operations with subversive, asymmetric, and non-linear methods. This type of conflict requires an instrumentalization of information vectors, which are subordinated to well-defined strategic interests. In this respect, the core of the hybrid conflict lies in the ability to speculate on the internal fragilities of the target states, be they political, social, or technological. They take place in a grey area of security, where the classic distinction between peace and belligerence is deliberately uncertain (NATO 2022), turning uncertainties into a tactical advantage.

The development of the analysis of the phenomenon requires the conceptual clarification of the notions present in the paper, disinformation, and FIMI. Disinformation is false or misleading information spread with the intent to deceive or cause harm. It can occur in the form of deliberately manufactured or manipulated audio/visual content, intentionally created conspiracy theories, or widespread rumors to harm or cause mistrust between citizens (Commons Social Change Library 2023).

As regards the Manipulation and Interference of Foreign Information (IMIF), it can no longer be seen as an isolated phenomenon, but as a systematic threat to the information balance and electoral processes. By deliberately eroding trust in the democratic apparatus, such actions directly target the integrity of the online environment. External actors manage to fracture social cohesion precisely by resorting to a mix of malicious tactics, techniques, and procedures (TTP), strategically disseminating narratives that alter public perception and weaken the foundation of the security of democratic countries (International IDEA).

The evolution from disinformation to FIMI marks a paradigm shift towards the analysis of coordinated manipulative behavior (EEAS 2025). This dynamic fits into the logic of hybrid and non-linear warfare, where the boundary between peace and conflict becomes intentionally uncertain, and national resilience is eroded by non-kinetic means (Global Security Review 2024). As mentioned in the Hybrid CoE report,

these aggressions are turning the entire society into a potential front, where aggression is no longer marked by a formal act of declaring war (Hybrid CoE 2023). State actors invest heavily in reflective control, manipulating the opponent's perception to get him to make decisions that serve his own strategic interests (NATO 2023).

The empowerment of the European institutions and NATO allies to adapt their defensive measures to combat and defend against disinformation facilitated the transition from a descriptive to an operational analysis. The DISARM framework allows handling operations to be broken down into a "kill chain" (attack chain) model, facilitating the reduction of FIMI incidents in their sequential phases (EEAS 2025). By mapping OCTs, ranging from bot creation and web domain acquisition to using AI to impersonate legitimate media sources, raw data is turned into strategic information (Commons Social Change Library 2023). This methodological approach underpins the transition to a proactive defense, giving Romania and European partners the ability to secure the digital space through rigorous attribution and classification methods.

Controlling the information field has thus surpassed the scope of public communication, becoming a critical component of the global information warfare (EEAS 2025). In this context, manipulation of information directly interferes in the internal affairs of countries, autocratic regimes using disinformation as a key non-kinetic activity against liberal democracies (Cenușă 2024). This systemic threat endangers the integrity of electoral processes and social cohesion through manipulative narratives that threaten the structure of the democratic community (International IDEA 2026).

Operations, architecture, and FIMI exposure framework

The strategic transition operated by the EEAS from the simple monitoring of disinformation content to the proactive identification of technical infrastructures, the introduction of which in 2025 was the FIMI Exposure Framework. It provides a systematic model of classification of sources of influence in four fundamental blocks, allowing decision makers to identify the degree of involvement of a foreign actor in disrupting the information space of a democratic state (EEAS 2025); in this case, the Russian Federation.

At the top of this pyramid are official state channels, representing the direct voice of governments through ministries or diplomatic representations, followed by state-controlled platforms, which are entities that benefit from public funding and government editorial direction, such as RT or Sputnik (EEAS 2025). Much more complex, however, is the basis of this architecture, consisting of channels with hidden state links, identified by technical indicators such as shared IPs (Internet Protocol) or shared hosting services, and non-attributed aligned channels. The latter represent the biggest security challenge, accounting for 76.5% of the investigated architecture,

as they allow the dissemination of malignant narratives without a proven formal link, facilitating "the washing of information" through networks that seem independent (EEAS 2025).

This classification is not only a theoretical exercise, but also a necessary tool for the securitization of digital space, given that FIMI actors systematically exploit anonymity to avoid legal and diplomatic liability. The analysis of manipulative behavior, rather than the truth of the content, allows the identification of coordinated aggression patterns aimed at societal stability (Proto et al. 2025). An eloquent example of this is the Russian Federation, because it is an actor that has developed this multi-level strategy to advance long-term geopolitical goals by creating instability among citizens of the target states (EEAS 2025).

Modern FIMI operations are characterized by outstanding technological adaptability, unfolding on multiple platforms to create "rooms of ideological echo". EEAS data indicates a massive concentration of activity on the X platform (formerly Twitter), which attracted 88% of detected incidents, due to the proliferation of CIB accounts (Coordinated Inauthentic Behavior) and the ease of generating fake accounts. The diversification of OCTs includes the use of AI to automate bot networks and create large-scale content, reducing operational costs for the aggressor. In 2024, the use of AI in creating audio-video deepfakes has become a current method to enhance the emotional impact of disinformation (EEAS 2025).

To increase the credibility of these narratives, aggressors frequently resort to impersonation, which refers to usurping the identity of legitimate media outlets such as the BBC and localizing the content. The latter involves the cultural and linguistic adaptation of messages to resonate with the specific vulnerabilities of the local public, transforming information into a weapon adapted to the national context. The operational analysis of these structures through DISARM enables proactive response to identify bullying in the planning phase (EEAS 2025).

Collective security and hybrid aggression

Current hybrid activities against NATO member states have moved past classic conflict models, prioritizing the psychological dismantling of public institutions over kinetic destruction. The goal is clear: to compromise the integrity of the rule of law using a calculated mix of disinformation and sabotage. This threat is distinct not just in its intent, but in its execution—the speed and magnitude of today's information activities are a direct result of the pervasive nature of digital platforms and the emergence of disruptive technological tools (NATO 2024).

From the Alliance's perspective, collective security in the 21st century requires an integrated approach centered on societal resilience. Resilience has become NATO's first line of defense, defined by the ability of societies to resist, adapt, and recover

quickly from attacks targeting key state functions (NATO 2024). This layered defense requires close cooperation in the public sector, the private sector, and civil society, and is not limited to post-incidental reactive responses, but invests in strengthening digital literacy and strategic partnerships with the EU. NATO's role in the current collective security architecture is to secure a stability framework that protects not only territorial integrity, but also information flows and democratic processes against any coordinated foreign interference (Homaniuk et al. 2026).

The analysis of Romania's vulnerabilities in the face of foreign manipulation actions requires a direct reporting to the security pillars defined by the National Defence Strategy for the Country 2025-2030. The document bases the process of securitization of the information space, defining disinformation and hybrid actions not only as risks but as direct threats to constitutional stability and social cohesion. An identified critical vulnerability is „the insufficient involvement of resilience in society in front of subversive narratives", which allows FIMI actors to explore citizens' mistrust in state institutions and European values. This weakness is amplified by a heterogeneous level of media literacy, which makes the population an easy target for emotional manipulation campaigns (CSAT 2025).

In the context of coordinated information manipulation, SNAT stresses that „the social and economic cleavages" inside Romania are transformed by Russian proxies into security breaches, used to generate polarization and undermine the national consensus regarding the Euro-Atlantic orientation. Another structural weakness mentioned in the document is „the vulnerability of digital critical infrastructures", which, in the absence of mechanisms for controlling false content, facilitates the rapid propagation of propagandistic messages. This technical vulnerability is associated with „dependence on external technological platforms", where recommendation algorithms may involuntarily favor the distribution of malignant narratives (CSAT 2025).

State actors also promote identity and sovereignty themes to provoke a political and military decision-making deadlock. Thus, the cognitive resilience of the population is a strategic objective, because the attack no longer targets only the physical infrastructure, but the decision-making process. SNAT proposes the transition from a reactive to a preventive approach, focusing on security education as a deterrent against hybrid aggression (CSAT 2025). This vulnerability is at the core of the current hybrid conflict on the eastern flank, requiring close collaboration between the institutions of force and civil society. Romania is a priority target on the eastern flank, as it is the target of complex FIMI operations that reflect the Russian doctrine of "information confrontation".

The role of the Russian Federation as an FIMI actor reflects the perception of the information space as an active area of combat, because it uses official tools (diplomacy, state media) and unofficial (proxy networks, troll farms), and due to these considerations, FIMI tactics are transformed into a major security concern

for Romania and the European Union. Operation Matryoshka is a sophisticated campaign of influence and disinformation coordinated by pro-Russian actors, identified and monitored intensively since 2023 and 2024. It works according to the principle of Russian dolls (a narrative hidden in another) and has as its main objective the flooding of the European information space with messages aimed at undermining support for Ukraine and creating mistrust in democratic institutions (EEAS 2024). The success of the operation Matryoshka is dependent on the degree of preexisting social fragmentation in Romania, because it is posted in the digital space with contradictory narratives, putting the Romanian state in a defensive posture.

In the current geostrategic framework, Romania ceased to be only a country of proximity, becoming a central pillar of the eastern flank and a priority target for hybrid operations carried out under the Russian security doctrine. The analysis reveals a transition to a permanent information confrontation, where information is used as a weapon to erode state cohesion and democratic stability. This strategy is based on the concept of "active measures", adapted to the digital era by the Russian intelligence services, whose purpose is not only to convince the audience of an untruth but to erode the very ability of the company to distinguish reality, thus causing a decision-making block at the political level (Global Security Review 2024; EEAS 2025).

Romania's vulnerability to FIMI is accentuated by the tactical exploitation of internal cleavage points. Russian proxies use content localization to adapt narratives to the national context, instrumenting themes that present NATO as a factor of insecurity. This ecosystem, exemplified by networks such as RT and Sputnik, uses "reflective" control techniques to manipulate public perception. By posting conflicting narratives about national security in the digital space, the aggressor leads Romanian institutions to adopt a defensive, reactive, and inefficient position, transforming a stable ally into an internal fractured state (Cenușă 2024). Moreover, the technique of "mirroring" through false "fact-checking" initiatives, such as the Global Fact-Checking Network, serves to discredit legitimate organizations and official media channels, leaving citizens in a dangerous informational vacuum (Prysiazhniuk 2025).

Romania's resilience cannot be ensured exclusively by technical regulations, but requires a cognitive immunization of the population through a "whole-of-society" approach. The EU has substantiated this response through the Digital Services Act (DSA), which imposes transparency obligations on digital platforms; through operational pillars such as the Rapid Alert System (RAS) and media literacy projects (EDMO) (EEAS 2025; CEDEM 2025). The effectiveness of external interference on the eastern flank is directly proportional to pre-existing cognitive vulnerabilities. The integrity of democratic processes depends on the transition from a "deterrence posture by denying" using political attribution and diplomatic sanctions in fora such as G7 and NATO (International IDEA 2026; NATO 2024). It is necessary to integrate DISARM-based behavioral monitoring into national defense strategies, thereby

ensuring that the information ecosystem is protected from non-linear warfare (Global Security Review 2024; EEAS 2025).

Conclusions

This article looked at the strategic transition from the simple management of disinformation to the FIMI framework, which is not just a terminological change but a fundamental redefinition of the concept. The analysis of the phenomenon confirms that the information space has become an active operational field, where geopolitical conflicts are carried out through digital tools of "reflective control". From the applied assessment on the national context and recent strategic documents, such as the National Defence Strategy for the Country 2025-2030 and Strategic Compass 2022, the results are derived that confirm the central hypothesis of the research: the adoption of the FIMI framework facilitates the transition from reactive to proactive defense by shifting the focus from content monitoring to identifying manipulative infrastructures.

A fundamental result of the research indicates that the FIMI Exposure Framework may allow Romania to go beyond the traditional "debunking" model in favor of early identification of attack infrastructures. Following the application of operational indicators, technical data, such as common IP addresses and bot networks, can be identified, allowing the phenomenon to be limited before it produces social effects. By applying the "kill chain" methodology within DISARM, institutions with responsibilities in national security can intervene in the early stages of planning. This approach transforms disinformation from a simple miscommunication into a complex hybrid attack, designed to break the cohesion of allied states and undermine the rules-based international order.

The research underlines that cognitive resilience, supported by the expertise of European and national institutions, is currently the fundamental basis of national defense. The results of the analysis indicate that the effectiveness of external interference is directly proportional to pre-existing cognitive vulnerabilities and to the heterogeneous level of media literacy of the population. This requires a paradigm shift, and media literacy needs to be integrated as the central pillar of national security, being the only sustainable barrier against attempts of "reflective" control aimed at decision-making.

The analysis applied to influence and disinformation campaigns, such as Matryoshka, demonstrated that Romania is facing an infrastructure of "permanent information confrontation. The success of Russian campaigns on national territory depends fundamentally on the degree of social fragmentation and the exploitation of radical narratives. Looking towards the strategic horizon of 2026, Romania's stability seems to depend fundamentally on the success of a strategy that is not limited to the institutional level, but to integrate civil society into the defense mechanism

against disinformation. It is not just a simple application of European rules, such as the Digital Services Act (DSA), but a much more complex articulation. This implies, on the one hand, the need for technology platforms to have a real responsibility in limiting disinformation messages and, on the other hand, creating an individual security culture. No regulation, however well-structured, can achieve its goal if there is a lack of public conviction in the reaction capacity of states. This solid trust is the foundation on which the resistance of a society is built in the face of information warfare tactics.

The strategic horizon of Romania depends on the ability to implement early warning mechanisms and facilitate an open dialogue between the state, academia, and the private sector. By adopting measures of "pre-bunking" (inoculation of information), the state can prevent the spread of false information by acting proactively in the face of hybrid destabilization strategies; more specifically, it can limit them before they produce profound effects in society. The FIMI analysis confirms that the information space is an operational field, where geopolitical conflicts are also carried out by digital means. Disinformation is no longer miscommunication, but a hybrid attack designed to break the cohesion of states and undermine the rules-based international order. In the absence of a culture of information resilience, digital vulnerabilities will continue to be exploited by state actors to turn the eastern flank into an area of strategic instability.

The limits of this research lie in the extreme volatility of the technical infrastructures used by FIMI actors, which can change their digital footprint faster than official reports can be updated. Moreover, an important conceptual limitation is the difficulty of isolating the impact of FIMI from organic social cleavages. The data suggest that the success of disinformation is often conditioned by pre-existing internal vulnerabilities, which makes the distinction between an authentic, albeit polarized, opinion and an artificially amplified narrative remain, in some cases, analytically subjective. More than just a theoretical assessment, future studies should assess the pragmatic effectiveness of the EU and NATO response in identifying sources of disinformation and their operational capabilities.

References

CEDEM (Centre for Democracy and Rule of Law). 2025. "What is Foreign Information Manipulation and Interference (FIMI) and how does it affect democracy?" https://cedem.org.ua/en/news/fimi/.

Cenușă, Denis. 2024. "Disinformation Narratives Driven or Beneficial to Russia: The Case of Moldova." Policy Paper, Eastern Europe Studies Centre (EESC), pp. 1–21. https://www.gssc.lt/wp-content/uploads/2024/04/v02_Cenusa_Russias-disinformation-in-Eastern_Europe_EN_A4.pdf.

Commons Social Change Library. 2023. "Disinformation and 7 Common Forms of Information Disorder." https://commonslibrary.org/disinformation-and-7-common-forms-of-information-disorder/.

CSAT (Consiliul Suprem de Apărare a Țării). 2025. "National Defence Strategy of the Country (SNAT) 2025-2030". https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

EEAS (European External Action Service). 2024. "2nd EEAS Report on Foreign Information Manipulation and Interference Threats". https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.

___. 2025. "3rd EEAS Report on Foreign Information Manipulation and Interference Threats." https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf.

European Council. 2022." A Strategic Compass for Security and Defence: For a European Union that protects its citizens, values and interests and contributes to international peace and security". https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

Global Security Review. 2024. „Hybrid and Non-Linear Warfare Systematically Erases the Divide Between War & Peace." https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/.

Homaniuk, Oleksandr, Yevheniia Vozniuk, Olena Borysiuk, Viktor Kobets, and Hryhorii Zeleniuk. 2026. "FIMI VS DISINFORMATION: IMPACT ON DIGITAL SECURITY AND PUBLIC ORDER IN THE EU." *Veredas do Direito* 23 (4): e234678. https://revista.domhelder.edu.br/index.php/veredas/article/view/4678/26742.

Hybrid CoE. 2023. "Trends in Hybrid Threats". https://www.hybridcoe.fi/wp-content/uploads/2023/04/CORE_comprehensive_resilience_ecosystem.pdf.

International IDEA. 2026. „Foreign Information Manipulation and Interference (FIMI)." https://www.idea.int/theme/foreign-information-manipulation-interference-fimi.

NATO. 2022. „Strategic Concept." Adopted by Heads of State and Government at the NATO Summit in Madrid. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2022_06/20220629-220629-strategic-concept.pdf.

___. 2024. "Countering Hybrid Threats." https://www.nato.int/en/what-we-do/deterrence-and-defence/countering-hybrid-threats.

NATO Allied Command Transformation. 2023. "Strategic Concept." https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf.

NATO CCDCOE. 2024. "Cyber Defence and Information Operations: Strategic Perspectives". https://ccdcoe.org/uploads/2024/05/CyCon_2024_book.pdf.

Proto, Lucas, Paula Lamoso-González and Luis Bouza García. 2025. "The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight." *Media and Communication* 13 (Article 9474): 1–15. https://doi.org/10.17645/mac.9474.

Prysiazhniuk, Marianna. 2025. "Strategic Narratives and Information Warfare: Russian FIMI Campaigns against Ukraine's Armed Forces in the Context of War and Societal Impact." *Culture. Society. Economy. Politics* 5 (1): 88–108. https://doi.org/10.2478/csep-2025-0007.

Stritzel, Holger. 2014. *Securitization Theory and the Copenhagen School.* In: *Security in Translation. New Security Challenges Series.* Palgrave Macmillan, London. https://doi.org/10.1057/9781137307576_2.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Assessing the Crime Control and Regional Security Responses: An Analytical Study of Operation Fagge Yamma, Nigeria

Akeem Ayanda ARABA, Ph.D.*
Opeyemi Muhammed TAOHEED**

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

Abstract

This study provides an analytical assessment of Operation Fagge Yamma, the joint military task force mandated to address escalating banditry, kidnapping, and terrorism in North-West Nigeria. The research employed a descriptive survey approach, utilizing a mixed-method design to gather both quantitative and qualitative data. A clustered/stratified sampling technique was used to administer 983 questionnaires and conduct interviews with a diverse population comprising Operation Fagge Yamma personnel, state-sponsored vigilance groups, community leaders, and general residents across purposively selected high-impact Local Government Areas in Zamfara, Katsina, and Kaduna States. The findings reveal a significant paradox: while the operation has achieved notable kinetic success in reducing the frequency of large-scale bandit attacks and kidnapping (RQ1), its overall effectiveness and long-term sustainability are severely undermined by critical systemic failures. These include a profound lack of inter-agency coordination and "turf wars" (RQ2), a persistent trust deficit with local communities driven by a lack of consultation, and perceptions of unprofessionalism and slow emergency response. The study concludes that while Operation Fagge Yamma is a necessary component of the regional security architecture, it cannot succeed as a purely kinetic, top-down intervention. It recommends a fundamental shift toward an integrated hybrid security model that formally mandates intelligence sharing and empowers state vigilance groups as partners to rebuild civil-military relations.

Keywords:
Operation Fagge Yamma (FansanYamma); Insecurity; Banditry; Regional security; Civil-Military Relations.

Article info
Received: 16 November 2025; Revised: 5 December 2025; Accepted: 22 January 2026; Available online: 8 April 2026

Citation: 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

Introduction

The fundamental responsibility of any government is to safeguard the lives and property of its citizens. This obligation is explicitly affirmed in the 1999 Constitution of the Federal Republic of Nigeria, which states that *"the security and welfare of the people shall be the primary purpose of government"* (Constitution of the Federal Republic of Nigeria 1999, Section 14(2)(b)). In modern societies, the state occupies a unique position as the central authority empowered to enforce laws, deploy coercive instruments, and maintain order, capacities that no other institution possesses (Weber 1946). However, growing crime rates and evolving forms of insecurity continue to challenge state capacity across the world, and Nigeria is no exception. Crime and violence have become pervasive features of the national landscape, undermining social stability, economic development, and citizens' sense of safety (Agunbiade 2024).

Nigeria has, over the past two decades, faced an unprecedented surge in security challenges ranging from insurgency, banditry, kidnapping, urban crime, and communal conflicts. According to the Global Terrorism Index (GTI), Nigeria consistently ranked among the top ten countries most affected by terrorism between 2015 and 2022 (Institute for Economics and Peace 2022). Additionally, the Nigeria Security Tracker (NST) has continuously documented rising incidents of violent crime, reporting thousands of fatalities annually from kidnapping, banditry, and communal attacks (Gavin 2023). These realities have compelled federal and state governments to experiment with a variety of security strategies, operational reforms, and collaborative regional initiatives aimed at mitigating violent crime.

In response to widening security gaps, Nigeria's security architecture includes a broad network of agencies such as the Nigeria Police Force (NPF), Department of State Services (DSS), Nigeria Security and Civil Defence Corps (NSCDC), and the Armed Forces, among others (Alemika 2013). However, persistent concerns over limited manpower, inadequate intelligence systems, and poor community trust have led to increasing advocacy for localized, community-driven security interventions (Abrahamsen and Williams 2017). Several regions have introduced subnational security structures designed to complement federal policing and improve rapid response to crime.

It is within this context that Operation Fagge Yamma (OPFY), which translates from Hausa to "Western Sweep", a Joint Task Force of the Nigerian military, emerged as a targeted security initiative aimed at strengthening crime control within the North-Western states of Nigeria. The operation was developed in response to escalating incidents of banditry, terrorism, street crime, gang violence, drug-related offences, and commercial-area insecurity. OPFY reflects a broader trend of community-

focused and intelligence-driven policing models, combining federal military operations with local collaboration to neutralize criminal elements (Omonobi et al. 2025). For instance, in its early phases, OPFY successfully coordinated efforts among the Nigerian Air Force, Army units, and local stakeholders to arrest over 90 suspects, recover weapons, and dismantle insurgent hideouts in Katsina and Sokoto states (Salman 2025).

Beyond Fagge, similar collaborative security models have demonstrated effectiveness in other Nigerian contexts. Operations like *Operation Puff Adder* in Zamfara and Kaduna involve coordinated military-police-community efforts to combat banditry, reduce kidnappings, and enhance intelligence gathering (Hills 2012; Mutum 2019). Such initiatives underscore the growing recognition that community participation and multi-agency coordination are essential for sustainable crime reduction.

A quick review of recent Nigerian news reports provides ample evidence of the prevailing state of insecurity in northern Nigeria, particularly in the north-west axis and surrounding communities. Instances of street crime, gang-related violence, kidnapping, drug trafficking, and attacks on commercial areas have become increasingly common (Rufus and Ogbe 2025; Alhassan 2026; Punch Editorial Board 2025). Nigeria continues to grapple with a complex and interconnected array of security challenges, ranging from local criminal networks to insurgent activities. These threats have affected nearly every aspect of social and economic life in the region, undermining community confidence and disrupting livelihoods. Operation Fagge Yamma primarily operates across the North-Western states of Zamfara, Sokoto, Katsina, Kebbi, and parts of Kaduna, with notable focus on LGAs such as Shinkafi, Bukkuyum, Anka, Tureta, Sabon Birni, and Chikun (Omonobi et al. 2025; Zubairu 2025). The operation has been instrumental in neutralizing armed criminal elements, rescuing kidnapped victims, recovering weapons, and disrupting insurgent and bandit networks in these areas (Nwannah 2025).

As a result, the primary focus of this study is to examine the concept and effectiveness of Operation Fagge Yamma, a collaborative security initiative launched in northern Nigeria to address rising crime and insecurity. The operation emerged in response to mounting pressure on government and security agencies to protect vulnerable communities and commercial centers from criminal activity. Coordinated by the Nigerian Armed Forces in partnership with local authorities and community stakeholders, Operation Fagge Yamma aims to enhance intelligence gathering, strengthen surveillance, and disrupt criminal networks (Maji 2025; Don 2025). In the contemporary Nigerian security context, adopting strategies that combine federal intervention with community-focused policing across multiple states and LGAs is critical for achieving regional stability, safeguarding lives and property, and fostering public trust in security institutions.

Research Questions

1. How effective has Operation Fagge Yamma been in reducing crime and improving public safety across the North-Western states of Nigeria?
2. What are the key challenges and achievements of Operation Fagge Yamma in coordinating multi-agency and community-focused security interventions in the Fagge axis and surrounding areas?

Objectives of the Study

1. The primary objective of this study is to evaluate the effectiveness of Operation Fagge Yamma in reducing crime and enhancing public safety across the North-Western states of Nigeria.
2. To identify and analyze the key challenges and successes of Operation Fagge Yamma in implementing multi-agency and community-focused security strategies in the Fagge axis and surrounding communities.

Literature Review

Security refers to the state or quality of being free from danger or threats. It encompasses the feeling of happiness and safety, devoid of worry or apprehension (Stevenson 2010). Crime prevention involves the implementation of strategies and measures aimed at diminishing the likelihood of crimes transpiring, as well as mitigating their potential adverse impacts on both individuals and society. These measures are designed to address the various root causes of crime, thereby reducing the incidence of criminal activities and alleviating the fear of crime within communities.

Nigeria is grappling with a security crisis primarily due to insufficient, misdirected, and ineffective security policies. The fundamental purpose of any nation is to ensure the safety and security of its inhabitants. However, Nigeria is currently confronted with a myriad of security challenges, including kidnapping and abduction incidents across various regions, rampant cases of robbery, human trafficking, and political assassinations, clashes between farmers and herdsmen, as well as broader national security issues.

Insecurity, reminiscent of the Hobbesian state of nature, characterized by a life described as solitary, poor, nasty, brutish, and short, reflects the current state of affairs in Nigeria. Similar to the concept articulated by Thomas Hobbes (1588–1679) in his work "Leviathan," published in 1651, wherein he depicts a state where the weak and common individuals are at the mercy of the strong, this tendency finds resonance in contemporary Nigeria. Hobbes argued that in the state of nature, where there is no established society, there is no concept of justice or injustice, and individuals possess an inherent right to all things, including the right to take others' lives. He posited that the State of Nature is a theoretical condition preceding the establishment of

'society' through a hypothetical 'Social Contract.' In this state, Hobbes observed that everyone acts out of self-interest, leading to what he termed a "war of all against all," a scenario mirroring the current situation in Nigeria.

According to Okoro (2020), herdsmen have wreaked havoc on entire communities, carrying out abductions, burning churches, murdering church leaders and congregants, attacking law enforcement personnel, committing rape, looting, and other egregious crimes. Meanwhile, the government's response to this crisis has been perceived as inadequate, posing a significant threat to both national security and development. The displacement of farmers from affected areas has led to a drastic reduction in agricultural output in Nigeria. This is evident from the scarcity of farm produce in both rural and urban markets across central Nigeria.

Scholars such as Adelakun (1990), Egwu (1990), Odekunle (2005), Adegoke (2016), Arinze (2010), and Uduo, Obaji-Akpet, and Okafor (2025) emphasize various factors contributing to the wave of insecurity in Nigeria. They assert that the Nigerian state's response to crises such as mass unemployment and petroleum shortages has exacerbated the country's crime situation. Additionally, poverty, declining incomes, low savings, high inflation rates, and political intolerance have all played a role in escalating insecurity nationwide.

According to Olakiitan (2016) and Offiah (2024), the government's failure to decisively address the issue of herdsmen attacks carries several implications for Nigeria. The fact that herdsmen now possess sophisticated weapons with which they freely target their perceived adversaries poses a grave threat to national security. This is exacerbated by the inability of security forces, including the police, to effectively counter the boldness and firepower exhibited by armed herdsmen.

According to Onifade, Imhonopi, and Urim (2013), the insecurity challenges in Nigeria have reached alarming levels, prompting widespread lamentation from the country's political and economic leaders, as well as the entire nation. The loss of loved ones and investments, along with the pervasive absence of safety in many parts of the country, has deeply affected the populace. The rapid rate at which innocent lives are being lost daily, coupled with the visible display of bottled-up frustration among citizens, remains a cause for concern.

The frequency of violent crimes, which include terrorism, kidnapping, armed robbery, banditry, suicide bombings, religious conflicts, ethnic clashes, politically motivated killings, and other criminal activities, has become a distressingly common aspect of life in Nigeria. The country's consistently low ranking in the Global Peace Index (GPI 2024), which places Nigeria among the least peaceful nations globally due to high levels of internal violence and societal insecurity, underscores the worsening state of insecurity within the nation (Institute for Economics and Peace 2024). Recent scholarly analysis further highlights the persistence and expansion of

banditry as a major driver of insecurity in Nigeria, with bandit attacks increasingly contributing to widespread violence, displacement, and economic disruption (Thompson 2025).

Olufolabo, Akintande, and Ekum (2015) have identified specific categories of crimes prevalent in both urban and rural areas of Nigeria. They highlight stealing, theft, and burglary as the most commonly committed crimes in many cities. Additionally, they point to factors such as illiteracy, broken families, association with delinquent peers, environmental vulnerabilities, and the perceived failure of law enforcement and judicial authorities in delivering justice as primary contributors to residential urban crime.

As early as the 1980s, reports of increasing crime rates in Nigeria were being documented (Times International 1985, 5). During this period, lives were no longer considered safe, and the nation grappled with insecurity challenges posed by offenders. However, the surge in crime witnessed in recent years is relatively more pronounced. The reality of insecurity, particularly stemming from criminal activities, has become increasingly apparent. The recent crime wave in Nigeria is characterized by escalating frequency, severity, and brutality. The emergence of security challenges such as kidnapping and clashes between farmers and herdsmen has resulted in the loss of numerous lives and properties.

METHODOLOGY AND DATA PRESENTATION

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. Data collection was conducted within selected Local Government Areas (LGAs) in the three chosen states, focusing on communities directly impacted by insecurity and the subsequent military intervention. The target population for the study comprised personnel of Operation Fagge Yamma (including military and police units), members of state-sponsored vigilance groups (like the Katsina Community Watch Corps), community leaders, and general residents from Zamfara, Katsina, and Kaduna States.A clustered/stratified sampling technique was employed to ensure proper representation of the different groups and locations involved in the study. This approach enabled the researcher to first cluster respondents based on their respective states and LGAs, and then stratify them into relevant categories such as security personnel, vigilance group members, community leaders, and residents. The sample size was determined using the Taro Yamane (1976) technique/method, as follows:

TABLE 1. Selected LGAs Based on High Impact of Banditry (Insecurity Hotspots)

State	Senatorial District	Selected LGA (Insecurity Hotspot)	Population (2006)
Zamfara	Zamfara North	Zurmi	293,837
	Zamfara Central	Gusau	383,162
	Zamfara West	Anka	142,280
Katsina	Katsina North	Jibia	169,748
	Katsina Central	Batsari	208,978
	Katsina South	Faskari	196,035
Kaduna	Kaduna North	Giwa	286,427
	Kaduna Central	BirninGwari	252,363
	Kaduna South	ZangonKataf	316,370
TOTAL			**2,249,200**

Source: National Population Commission of Nigeria 2006; Compiled from Security Reports (2023-2025).

$n=N/ (1+N (e)^2$
Or

$$n= \frac{N}{1 + N (e)^2}$$

Where
n= signifies the sample size
N= signifies the population under study
e= signifies the margin error (it could be 0.10, 0.05 or 0.01)

Zamfara (293,837+ 383,162 + 142,280= 819,279)
$n=N/(1+N (e)^2$
n= 819,279 / (1+ 819,279 (0.05)2
n= 819,279 / (1+ 819,279 (0.0025)
n= 819,279 / (1+2048.1975)
n= 819,279 / 2049.1975
n=399.8 or 400

Katsina (169,748 + 208,978 + 196,035 = 574,761)
$n=N/(1+N (e)^2$
n= 574,761 / (1+ 574,761 (0.05)2
n= 574,761 / (1+ 574,761 (0.0025)
n= 574,761 / (1+1436.9025)
n= 574,761 / 1447.9025
n=399.7 or 400

Kaduna
$n=N/ (1+N (e)^2$
n= 855,160 / (1+ 855,160 (0.05)2
n=855,160 / (1+ 855,160 (0.0025)
n= 855,160 / (1+2137.9)
n= 855,160 / 2138.9
n=399.8 or 400

The sample size for this study was determined through stratified sampling technique to be 1200 respondents for the questionnaire, comprising 400 individuals each from Zamfara, Katsina and Kaduna States. The questionnaire comprised two sections: Section A included demographic questions, while Section B addressed inquiries pertinent to the research topic. Responses were structured using a 5-point Likert scale format, ranging from "strongly agree" to "strongly disagree."A total of 1200 questionnaires were distributed, of which 983 were completed and returned accurately.

DATA PRESENTATION, ANALYSIS AND DISCUSSION

RESULTS AND FINDINGS

TABLE 2. Demographic Characteristics of Respondents

CHARACTERISTICS	CATEGORY	FREQUENCY	PERCENTAGE
Gender	Male	627	64%
	Female	356	36%
Age Group	21-30	290	30%
	31-40	335	34%
	41-50	198	20%
	51 and above	160	16%
Marital Status	Single	393	40%
	Married	590	60%
Target population	Operation Fagge Yamma Personnel	246	25%
	State-sponsored Vigilance Groups	147	15%
	Community Leaders	98	10%
	General Residents (Zamfara, Katsina, Kaduna States)	492	50%

Source: Survey data collected from fieldwork, 2025.

Table 2 above presents the demographic characteristics of the respondents. Among the 983 participants, 627 (64%) are male, while 356 (36%) are female. Additionally, the table reveals that the majority of respondents fall within the age bracket of 31-40, comprising 335 individuals (34%). Those aged 21-30 account for 290 respondents (30%), while 41-50-year-olds constitute 198 individuals (20%). Respondents aged 51 years and above represent the smallest proportion, with 160 individuals (16%). Regarding the target population, 246 respondents (25%) are personnel of Operation Fagge Yamma (including military and police units), 147 respondents (15%) are members of state-sponsored vigilance groups (such as the Katsina Community Watch Corps), 98 respondents (10%) are community leaders, and 492 respondents (50%) are general residents from Zamfara, Katsina, and Kaduna States.

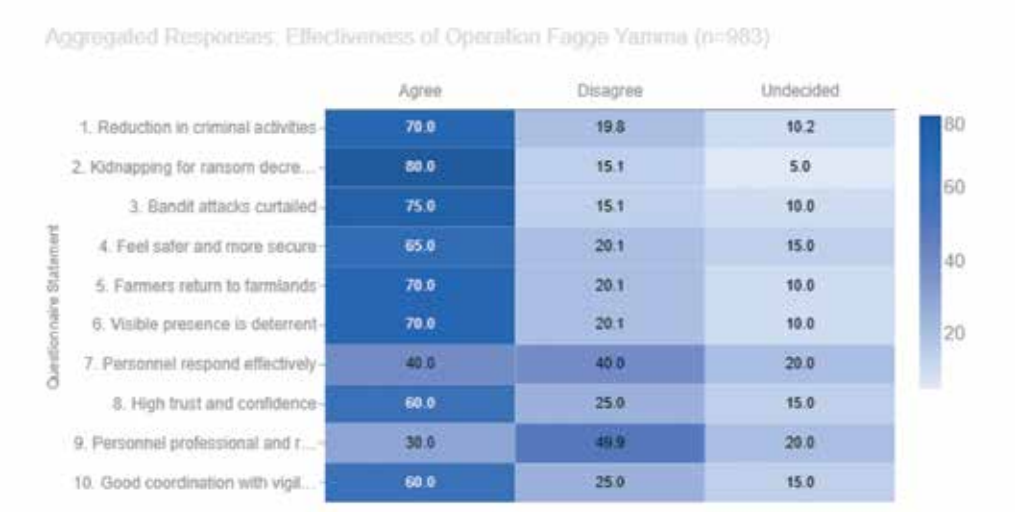

Figure 1 Effectiveness of Operation Fagge Yamma in Reducing Crime and Improving Public Safety

Source: Field Survey 2025

Research Question One: How effective has Operation Fagge Yamma been in reducing crime and improving public safety across the North-Western states of Nigeria?

NOTE: SA+A=Agreed; D+SD= Disagreed

Figure 1 presents the findings regarding the effectiveness of Operation Fagge Yamma in reducing crime and improving public safety. It indicates that a majority of 393 respondents (40%) strongly agreed that there has been a noticeable reduction in overall criminal activities, while 295 respondents (30%) agreed. However, 442 respondents (45%) strongly agreed that the rate of kidnapping for ransom has significantly decreased, with 344 respondents (35%) agreeing. Additionally, 344 respondents (35%) strongly agreed that attacks by armed bandits on villages have been curtailed, and 393 respondents (40%) agreed.

Furthermore, 295 respondents (30%) strongly agreed and 344 respondents (35%) agreed that they feel safer and more secure in their daily lives. Moreover, the table reveals that 393 respondents (40%), representing the majority, strongly agreed that farmers can return to their farmlands with less fear, while 295 respondents (30%) agreed. In addition, 295 respondents (30%) strongly agreed and 393 respondents (40%) agreed that the visible presence of personnel has served as a strong deterrent to crime.

Additionally, 147 respondents (15%) strongly agreed and 246 respondents (25%) agreed that personnel respond quickly and effectively to incidents, indicating mixed perceptions about response efficiency. Furthermore, 246 respondents (25%) strongly agreed and 344 respondents (35%) agreed that there is a high level of trust and confidence in the operation. Moreover, the table indicates that 98 respondents (10%) strongly agreed and 197 respondents (20%) agreed that personnel conduct their duties professionally and respect rights, while 295 respondents (30%) disagreed.

Additionally, 197 respondents (20%) strongly agreed and 393 respondents (40%) agreed that there is good coordination with state vigilance groups to enhance operational effectiveness. Overall, the findings suggest that Operation Fagge Yamma is perceived as largely effective in reducing crime and improving public safety, although areas such as personnel response and professional conduct may require further attention.

Research Question Two: What are the key challenges and successes of Operation Fagge Yamma in coordinating multi-agency and community-focused security interventions in the Fagge axis and surrounding areas?

Figure 2 Challenges and Successes of Coordination
Source: Field Survey 2025

Figure 2 presents the findings regarding the challenges and successes of coordination in Operation Fagge Yamma. It indicates that 147 respondents (15%) strongly agreed and 295 respondents (30%) agreed that the operation has successfully built strong,

trusting relationships with community leaders, while 295 respondents (30%) disagreed. However, only 98 respondents (10%) strongly agreed and 197 respondents (20%) agreed that effective and timely intelligence sharing occurs between agencies, suggesting some gaps in inter-agency collaboration.

Furthermore, 344 respondents (35%) strongly agreed and 393 respondents (40%) agreed that rivalry or "turf wars" between agencies have hindered operations, highlighting inter-agency friction as a significant challenge. Moreover, 98 respondents (10%) strongly agreed and 246 respondents (25%) agreed that communities actively provide timely intelligence, while 344 respondents (35%) disagreed, indicating limited community participation in reporting.

Additionally, 147 respondents (15%) strongly agreed and 344 respondents (35%) agreed that state vigilance groups have been successfully integrated into planning, showing moderate success in coordination. The table also reveals that 295 respondents (30%) strongly agreed and 295 respondents (30%) agreed that a lack of trust between residents and personnel remains a major challenge.

In terms of communication, 246 respondents (25%) strongly agreed and 344 respondents (35%) agreed that poor communication between Operation Fagge Yamma and the Police is an ongoing issue. Conversely, consultation with community stakeholders appears limited, as only 98 respondents (10%) strongly agreed and 147 respondents (15%) agreed that personnel regularly consult with community stakeholders, while 393 respondents (40%) disagreed.

Joint patrols with vigilantes were perceived as a successful strategy, with 246 respondents (25%) strongly agreeing and 393 respondents (40%) agreeing. Finally, language and cultural barriers were reported as a coordination challenge, with 197 respondents (20%) strongly agreeing and 344 respondents (35%) agreeing.

DISCUSSION ON MAJOR FINDINGS

Research Question 1

To what extent has Operation Fagge Yamma been effective in reducing crime and improving public safety in North-West Nigeria?

The insecurity challenges in Nigeria, which had reached "alarming levels" (Onifade, Imhonopi, and Urim 2013), prompted the large-scale intervention of Operation Fagge Yamma. The findings from this study's survey data indicate a significant, though nuanced, public perception of the operation's effectiveness.

From the gathered data (Table 1), the operation's primary success is seen in its kinetic impact on major crimes. A striking majority of respondents, 80.0% (442 'Strongly Agree' and 344 'Agree'), perceived a significant decrease in the rate of kidnapping for ransom (Q2). This was corroborated by a similar 75.0% (344 'Strongly Agree'

and 393 'Agree') who agreed that attacks by armed bandits on villages have been curtailed (Q3). This suggests that the operation's "hard power" approach—deploying a joint task force to clear and hold territory, has effectively disrupted the bandits' core economic activities.

This quantitative finding was supported by qualitative data from the field. During an interview, a community leader in Zurmi LGA, Zamfara State, stated:

> Before Operation Fagge Yamma was launched, the road from here to KauraNamoda was a death trap. We were paying levies to bandits just to exist. Now, with the army's super camp, we see their patrols, and the fear has reduced. We can at least go to the market.

This sentiment was further echoed by the 70.0% of respondents (Table 1, Q5) who agreed that the operation's presence has allowed farmers to begin returning to their farmlands. However, this success is tempered by significant challenges in responsiveness and professionalism. A major area of concern was identified in Q7, where 40.0% of respondents (295 'Disagree' and 98 'Strongly Disagree') felt that personnel do not respond quickly or effectively to security incidents.

This suggests a "garrison" model of security, where personnel are effective in their immediate vicinity (patrols, checkpoints) but slow to react to emergencies in remote or outlying areas. This perception of poor responsiveness is dangerously coupled with findings on professionalism. A critical finding in Q9 revealed that nearly 50.0% of respondents (295 'Disagree' and 196 'Strongly Disagree') believe the personnel do not conduct their duties professionally or with respect for rights.

The clustered/stratified nature of the sample was particularly revealing here. Analysis showed that 'General Residents' in the survey were significantly more likely to report negative perceptions on Q9 than 'Community Leaders' or 'Security Personnel', indicating a dangerous gap in trust between the military and the populace it is meant to protect.

Research Question 2

What are the key challenges and successes of Operation Fagge Yamma in coordinating multi-agency and community-focused security interventions?

Ambali & Araba (2020) argue that state-level corps are essential for effective community policing. The success of a federal operation like Fagge Yamma, therefore, depends heavily on its ability to coordinate with state agencies and local communities.

The findings from this study (Table 2) suggest that inter-agency coordination is the single greatest challenge to the operation's long-term success. An overwhelming 75.0% of respondents (344 'Strongly Agree' and 393 'Agree') agreed that rivalry or "turf wars" between agencies actively hinder security operations (Q3). This is not

just a perception; it has operational consequences. A further 60.0% (344 'Disagree' and 98 'Strongly Disagree') felt there was no effective and timely intelligence sharing between agencies (Q2).

This "silo" effect was a dominant theme in qualitative interviews. A Zonal Coordinator with the Katsina Community Watch Corps (CWC) stated:

> We are the ones who live here. We know the informants, we know the terrain, we know the families. We will bring credible intelligence to the army, and they will ignore it. Then they will act on their own, often too late, or they will take the credit for an operation we initiated. There is no partnership, only hierarchy.

This statement is particularly poignant when contrasted with the data from Q9 (Table 2), where 65.0% of respondents (246 'Strongly Agree' and 393 'Agree') believed that joint patrols (when they do happen) are a successful strategy. This highlights a major missed opportunity: while the public sees the *value* in cooperation, this cooperation is being undermined by institutional friction.

This coordination failure extends to the community level. The data (Table 2, Q6) shows that 60.0% of respondents (295 'Strongly Agree' and 295 'Agree') believe a lack of trust remains a major challenge. This trust deficit is directly linked to a lack of consultation, as 60.1% (393 'Disagree' and 198 'Strongly Disagree') reported that Operation Fagge Yamma personnel do not regularly consult community stakeholders (Q8).

An officer with Operation Fagge Yamma, speaking on condition of anonymity, provided a counter-perspective that explains this gap:

> Consultation is a risk. We have seen operations fail because the community was compromised. Bandits have informants everywhere. Our priority is operational security. We cannot always tell the community leaders our plans.

This creates a dangerous, self-perpetuating cycle: The military, citing security, withholds consultation. The community, feeling disrespected and profiled (as seen in Q9, Table 4.1), withholds timely intelligence. This forces the military to rely on more aggressive, less-informed tactics, which further erodes community trust.

Recommendations

1. The findings from this study revealed that a primary challenge to regional security is the persistence of inter-agency rivalry and poor intelligence sharing. Therefore, the Federal Government, through the Office of the National Security Adviser (ONSA), should mandate the creation of a fused intelligence and operational cell for the North-West. This cell must integrate personnel from Operation Fagge Yamma (Military), the Nigeria Police Force, the Department of State Services (DSS), and,

critically, the state-sponsored vigilance groups (like the Katsina CWC) as equal partners in planning and execution. This formal structure would replace the current ad-hoc cooperation and address the "turf wars" identified in the findings, ensuring that the successful model of joint patrols is institutionalized.

2. According to Section 14(2) of the Constitution of the Federal Republic of Nigeria, the primary responsibility of government is the welfare and security of its citizens. This study found a significant trust deficit between Operation Fagge Yamma personnel and the general populace, driven by a lack of consultation and perceived unprofessionalism. To alter this current state of facts, the military command should institutionalize Civil-Military Coordination (CIMIC) units within each operational "super camp." This unit's sole mandate should be non-kinetic: to serve as permanent liaison with community leaders, traditional rulers, and residents, thereby creating a formal, safe channel for dialogue and local intelligence gathering. This directly addresses the "lack of consultation" finding and is the only sustainable path to shifting the operation from an "enemy-centric" to a "community-centric" model. The findings indicate that while state vigilance groups possess invaluable local intelligence and trust, they are often outgunned. The Federal and State governments must collaborate to create a formal framework for equipping and training these state-sponsored corps. Providing them with communication gadgets, protective gear, and standardized training (including some on human rights and rules of engagement) would elevate them from a subordinate, local force to a capable, professional partner for Operation Fagge Yamma. This would enhance the security architecture by creating a more effective "hybrid force" capable of holding territory after the military's kinetic operations.

Conclusion

Insecurity has long plagued Nigeria's North-West, driven by vast ungoverned spaces, porous borders, and entrenched armed banditry. The Federal Government's conventional security forces, centralized and rigid, have struggled to address these complex threats, especially given the region's vast and rugged terrain.With rising kidnappings and large-scale attacks, it has become clear that traditional security agencies alone are not enough. Operation Fagge Yamma was launched as a direct military response and a confidence-building measure for communities in Zamfara, Katsina, and Kaduna states. However, this operation cannot replace local policing or community intelligence, it must work alongside them. While it has had some success in reducing large-scale attacks, long-term security depends on improving coordination between agencies and building trust with communities. Operation Fagge Yamma is a crucial part of a hybrid security approach that blends federal military power with local, community-driven efforts.

References

Abrahamsen, R., and M. Williams. 2017. *Security Beyond the State: Private Security in International Politics.* Cambridge: Cambridge University Press.

Adegoke, Niyi. 2016. "Improving government security policy for sustainable development in Lagos State." *Journal of Sustainable Development in Africa* 18(4): 97-107. https://jsd-africa.com/Jsda/Vol18No4-Fall21016/PDF/Improving%20Government%20Security%20Policy.Niyi%20Adegoke.pdf.

Adelakun, Ebiyoma**.** 1990. "Crime as Social Adjustment to Structural Adjustment Programme." Paper presented at a Seminar for Crime and Crime Control in Nigeria, University of Jos. November 26.

Agunbiade, O. 2024. Crime, violence and national development in Nigeria. *African Journal of Social Sciences and Humanities Research* 7(2): 166–181. https://doi.org/10.52589/AJSSHR-PGKPNW8K.

Alemika, E.E.O. 2024. *Intelligence services and national security in Nigeria*. In O. Oshita, I. Alumona, & F. Onwubuemeli (Eds.), *Contemporary security issues in Nigeria* (pp. 157–179). London: Routledge.

Alhassan, Abdullahi. 2026. "Mass kidnapping at Kaduna churches adds to pressure on Nigeria." *Reuters.* https://www.reuters.com/business/media-telecom/mass-kidnapping-kaduna-churches-adds-pressure-nigeria-2026-01-20/.

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.

Arinze, P.E. 2010. ~An evaluation of the effect of armed robbery on Nigeria economy.~ *Transcampus Journal of Research in National Development* 8(2).

Constitution of the Federal Republic of Nigeria. 1999. https://nigeriarights.gov.ng/files/constitution.pdf.

Don, Hagxy. 2025. "Bello Turji's ally neutralized in Sokoto airstrike — Nigerian Army confirms." *Abuja Network News.* https://www.abujanetworknews.com.ng/2025/05/bello-turjis-ally-neutralized-in-sokoto.html.

Egwu, S. 1990. "The political economy of urban crime in Nigeria." *Africa Development* 15(1): 93–116. https://www.jstor.org/stable/24486893.

Gavin, Michelle. 2023. "Nigeria security tracker." *Council on Foreign Relations.* https://www.cfr.org/nigeria/nigeria-security-tracker/p29483.

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.

Hobbes, T. 1651. *Leviathan, or The matter, forme and power of a common-wealth ecclesiasticall and civill.* London: Andrew Crooke. https://www.gutenberg.org/ebooks/3207.

Institute for Economics and Peace. 2022. *Global Terrorism Index 2022: Measuring the impact of terrorism*. https://www.visionofhumanity.org/wp-content/uploads/2022/03/GTI-2022-web-04112022.pdf.

___. 2024. *Global peace index 2024: Measuring peace in a complex world.* https://www.economicsandpeace.org/wp-content/uploads/2024/06/GPI-2024-web.pdf.

Maji, Faith Awa. 2025. "Air Chief vows to eliminate insurgents, bolster national security." *BusinessDay.* https://businessday.ng/news/article/air-chief-vows-to-eliminate-insurgents-bolster-national-security/.

Mutum, Ronald. 2019. "Insecurity: IGP launches Operation Puff Adder." *Daily Trust.* https://dailytrust.com/insecurity-igp-launches-operation-puff-adder/.

National Population Commission of Nigeria. 2006. *Population and housing census of the Federal Republic of Nigeria 2006.* Abuja: National Population Commission. https://www.nationalpopulation.gov.ng/publications/census-2006.

Nwannah Ifeanyichukwu. 2025. "Troops neutralise bandits, rescue nine kidnap victims." *The Guardian Nigeria.* https://guardian.ng/news/nigeria/metro/troops-neutralise-bandits-rescue-nine-kidnap-victims/.

Odekunle, Femi. 2005. "Overview of Policing in Nigeria: Problems and Suggestions." In *Crime and Policing in Nigeria: Challenges and Options* edited by E.O. Alemika & I.C. Chukwuma,. 22-34. Lagos: Network on Police Reform in Nigeria (NOPRIN)/CLEEN Foundation.

Offiah, Anthony. 2024. "The menace of Fulani herdsmen in Nigeria: A threat to national security." *Journal of African Resilience & Advancement Research* 6(2). https://hummingbirdjournals.com/jarar/article/view/236.

Okoro, John Peter. 2020. Herdsmen–farmers' conflict: Implication on national development (Nigeria in perspective). *International Journal of Scientific & Engineering Research* 11(2): 808-820.

Olakiitan, Victor. 2016. "OkeAko Fulani herdsmen invasion: Still reeling from the shock" *Thisdaylive.* https://www.thisdaylive.com/2016/06/05/oko-ako-fulani-herdsmen-invasion-still-reeling-from-the-shock/.

Olufolabo, O.O, O.J. Akintande, and M.I. Ekum. 2015. "Analyzing the Distribution of Crimes in Oyo State (Nigeria) using Principal Component Analysis (PCA)." *IOSR Journal of Mathematics* 11 (3): 90-96. https://www.iosrjournals.org/iosr-jm/papers/Vol11-issue3/Version-1/L011319096.pdf.

Omonobi, K., W. Mosadomi, B. Bello, N. Marama, and H. Aliyu. 2025. "Nigeria: Insecurity – NAF strikes kill terrorists, bandits in Borno, Kwara, Katsina, others." *Vanguard.* https://www.vanguardngr.com/2025/11/insecurity-naf-strikes-kill-terrorists-bandits-in-borno-kwara-katsina-others/.

Onifade, C., D. Imhonopi, and U.M. Urim. 2013. "Addressing the Insecurity Challenges in Nigeria; the Imperative of Moral Values and Virtue Ethics. *Global journal of Human Science and Political Science* 13 (2): 52-63. https://www.researchgate.net/publication/263132433_Addressing_the_Insecurity_Challenge_in_Nigeria_The_Imperative_of_Moral_Values_and_Virtue_Ethics_Global_Journal_of_Human_Social_Science_GJHSS-F13253-63.

Punch Editorial Board. 2025. "Bandits kidnap 490 in two week rampage." *Punch Newspapers.* https://punchng.com/bandits-kidnap-490-in-two-week-rampage.

Rufus, Anthony Israel, and Ekoja Bernard Ogbe. 2025. "The rise of banditry in Northwest Nigeria: Examining the security implications and pathways to stability." *Kashere Journal of Politics and International Relations* 3(1): 22–25. https://fukashere.edu.ng/journals.fukashere.edu.ng/index.php/kjpir/article/download/399/331.

Salman, Animashaun. 2025. "Troops dismantle camps, arrest collaborators in Sokoto and Katsina – Theatre Commander." *Punch Newspapers.* https://punchng.com/were-not-here-to-party-army-commander-vows-to-crush-banditry/.

Stevenson, Angus. 2010. *Oxford dictionary of English* (3rd ed.). Oxford: Oxford University Press. https://www.oxfordreference.com/view/10.1093/acref/9780199571123.001.0001/acref-9780199571123.

Times International. 1985. "Crime: Can Death Penalty Deter Criminals?" 4 noiembrie 1985, p. 5.

Thompson Sara. 2025. "Exploring banditry in Nigeria." *Security Journal* 38, Article 28. https://doi.org/10.1057/s41284-025-00477-1.

Uduo, Thomas Achu, Immaculata Ofu Obaji-Akpet, and Mary Ogochukwu Okafor. 2025. "The nexus between organised crime, insecurity, and poverty in Nigeria: An exploratory analysis." *East African Journal of Arts and Social Sciences* 8(2): 129-144. https://doi.org/10.37284/eajass.8.2.3031.

Weber, Max. 1946. *Politics as a Vocation.* In H.H. Gerth & C. Wright Mills (Eds.), *From Max Weber: Essays in Sociology.* Oxford University Press.

Yamane, T. 1967. *Statistics: An introductory analysis* (2nd ed.). New York: Harper and Row. https://archive.org/details/statisticsintrod00yama.

Zubairu, Yusuf. 2025. "Operation FANSAN Yamma records major success in Zamfara, Sokoto." *Radio Nigeria Kaduna.* https://www.radionigeriakaduna.gov.ng/2025/09/11/operation-fansan-yamma-records-major-success-in-zamfara-sokoto/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

From Secret Diplomacy to Institutional Interaction: Intelligence Services and Intelligence Diplomacy in Conflict Resolution

Assoc. Prof. Ali GÖK, Ph.D.*

*Gaziantep University, Islahiye Faculty of Economics and Administrative Sciences, Department of Public Administration, Gaziantep, Türkiye
e-mail: aligok86@gmail.com
https://orcid.org/0000-0002-0734-459X

Abstract

Increasing expectations of transparency in formal diplomacy often limit the effectiveness of official channels, particularly in sensitive strategic matters, leading states to rely on the less visible, yet highly flexible, mechanism of intelligence diplomacy. Moreover, traditional diplomatic tools have struggled to resolve post-9/11 conflicts, which are characterized by hybrid warfare, gray zones, and the prominence of non-state actors. To address these challenges, governments increasingly utilize intelligence services not merely for information gathering but as primary actors in conflict resolution. This study investigates the effectiveness of intelligence diplomacy in conflict resolution processes by employing a qualitative multiple case study design based on open sources. The cases were selected to determine whether the outcomes of such initiatives are driven by idiosyncratic conditions or systematic structural factors. The analysis focuses on three core activities: covert negotiations, mediation, and information sharing. The findings suggest that intelligence diplomacy has evolved from a supportive auxiliary function into a structural necessity, providing a critical alternative where formal diplomacy fails. The study concludes that intelligence services effectively navigate the complexities of modern conflicts by establishing initial contact and sustaining dialogue in environments where official diplomatic presence is limited or impossible.

Keywords:
Conflict Resolution; Diplomacy; Intelligence Services; Intelligence Diplomacy; Secret Diplomacy; Gray Zone.

Article info
Received: 19 December 2025; Revised: 20 January 2026; Accepted: 17 February 2026; Available online: 8 April 2026

Citation: Gök, A. 2026. "From Secret Diplomacy to Institutional Interaction: Intelligence Services and Intelligence Diplomacy in Conflict Resolution." *Bulletin of "Carol I" National Defence University*, 15(1): 56-76. https://doi.org/10.53477/2284-9378-26-04

In the dynamic and unpredictable world of international relations, uncertainty is an ever-present reality. Governments must constantly assess the potential benefits and risks of their decisions, taking into account the possibility of unanticipated events that could derail their plans and have far-reaching consequences. Risk assessment and the capacity to strategize according to the current situation are among the main tools for minimizing the potential negative consequences of foreign policy (Debo 2023, 74).

In this framework, diplomacy and intelligence activities have historically functioned in a complementary manner to prevent or mitigate these risks. According to the traditional approach, the information provided by intelligence services has been supportive of diplomatic processes. Traditionally, these organizations are not directly decisive in the foreign policy-making process and are not considered institutions with decision-making or implementation authority. After the Cold War, increasing spheres of influence and technological developments have transformed diplomacy into a more complex structure concentrated on data analysis and reinforced by intelligence services. In other words, in today's world, where threats have become hybrid and traditional security understanding and diplomacy methods are insufficient, intelligence services have started to exceed their traditional roles and become institutionalized diplomatic actors. The role of intelligence services in this shifting approach to diplomacy has been conceptualized in the specialized literature as "intelligence diplomacy". Intelligence diplomacy is a type of diplomacy in which intelligence services, as foreign policy actors, conduct direct diplomatic activities, often in secret. These activities include, mainly, negotiation, mediation, and information sharing.

Although conflict resolution is a common problem of intelligence and diplomacy, the diplomatic efforts of intelligence services in the post 9/11 conflicts have been one of the important fields of study of intelligence diplomacy.
Governments employ intelligence services as part of conflict resolution, and these actors not only gather information on the parties but also work to strengthen the basis for reconciliation and directly determine strategy as a foreign policy actor. The role of intelligence services in conflict resolution is, in fact, the essence of intelligence diplomacy and can greatly contribute to conflict resolution when used effectively. Richard Gowan, the International Crisis Group's UN Director, explained this new process in conflict resolution by stating that "heads of intelligence services are increasingly replacing diplomats in peacemaking and mediation efforts and intelligence diplomacy is replacing the UN" (Athanasiadis 2024).

So, is intelligence diplomacy increasingly replacing formal diplomacy in conflict resolution? This study examines the hypothesis that intelligence diplomacy (the use of intelligence entities as primary actors in conflict resolution) is more suitable for resolving or mitigating conflicts in the post-9/11 era; it aims to demonstrate that this method is more effective compared to traditional methods. In this study, first of

all, the transformation of diplomacy in line with the dynamics of the international system and technological developments, and the position of intelligence services in this transformation process will be revealed. The final section will analyze the role of intelligence diplomacy in conflict resolution, focusing on multiple contemporary conflicts that have emerged in different contexts post 9/11.

This study investigates the effectiveness of intelligence diplomacy in conflict resolution processes by employing a qualitative multiple case study design. The methodological rationale for adopting this design is to discern whether the outcomes of such diplomatic initiatives are driven by idiosyncratic (case-specific) conditions or systematic structural factors. Given the inherent secrecy of intelligence operations and the classification of official archives, data collection is significantly constrained. To mitigate this methodological challenge, a systematic data collection strategy based on open-source techniques is employed.

Case selection was guided by the following criteria: (a) the conflicts that occurred in the post-9/11 era, (b) the intelligence service functioned as the "primary diplomatic actor" rather than a supportive element, and (c) the cases represent distinct geopolitical contexts (State-to-State and State-to-Non-State Actor). This diversity enables an analysis of the operational mechanisms of intelligence diplomacy across varying political contexts. Accordingly, the selected cases are analyzed within the framework of the primary activities of intelligence diplomacy: covert negotiations, mediation, and information sharing (cooperation).

The Transformation of Diplomacy: Alternative Methods

Diplomacy is only one of the tools a government uses to implement its foreign policy strategy. There are many different definitions of the concept. Diplomacy can be defined as "the system and art of communication between actors" (Wight 1978, 113). According to another definition, diplomacy involves "the formulation and implementation of a state's foreign policy" (Bull 2002, 158). Morgenthau's statement that "the method of establishing the preconditions for a lasting peace is called peace through compromise and its instrument is diplomacy" is also noteworthy (Morgenthau 1948, 419). These definitions generally consider diplomacy as the negotiated management of international relations.

More generally, diplomacy is the process of gathering and evaluating information about the international environment and formulating alternative policy strategies. According to the 1961 Vienna Convention, Article 3, diplomacy is the process of formulating and implementing alternative policy strategies through negotiations documented or endorsed by gathering and evaluating information about the international environment. Implementation involves the process of communicating the agreed foreign policy strategy to other governments and societies and, when appropriate, securing their cooperation towards the relevant policy, usually through

persuasion or other forms of coercion. Diplomacy is used not only in official relations between states, but also in the relations of other political actors with a certain position in world politics. Political groups that are not recognized as states sometimes communicate with states and/or other such groups through intelligence services. As Bull puts it, diplomacy is not limited to sovereign states, but it is one of the main means of communication of the "international community" (Bull 2002, 157-158)

There are many spaces and forms for diplomacy. It can take place bilaterally, multilaterally, in a formal or informal setting, and can be conducted publicly or, more often, in secret. At this point, especially secret diplomacy is an important way of achieving foreign policy objectives. Secret diplomacy is seen as the process of obtaining information from certain individuals and groups, concealing it from all or some, and/or sharing it with others. Depending on the situation, information obtained openly or secretly can be manipulated, distorted, or propagandized to suit national interests or foreign policy objectives. At this point, the fact that secret diplomacy can be covert blurs the boundaries between it and intelligence activities (Murray 2016, 15, 20-21).

Throughout history, diplomacy has been the main factor in international relations. The beginning of this system has two pillars: resident embassies and conferences. Abandoning the temporary method of dispatching special envoys during specific crises, states began to establish permanent embassies in each other's capitals - a practice that originated in 15th-century Italy and rapidly spread across Europe as a significant means of diplomatic communication (Wight 1978, 113). In the final decades of the 18th century, most European states had specialized departments and ministries for foreign policy management. The Congress of Vienna in 1815 provided an opportunity to review and adjust established diplomatic practices. As a result, there was a more than superficial order in the conduct of international politics, and the aftermath of World War I came to be known as the "new diplomacy." Indeed, it is possible to say that an important system of international relations developed in the 100 years following the Napoleonic Wars, particularly in Europe (Hamilton and Langhorne 2011, 93-94).

However, looking at the history of diplomacy, "old diplomacy" is actually not that old. It started in the Renaissance and lasted until World War I. Diplomacy's strengths lie in its ability to maintain order and peace, establish normative frameworks, and engage in self-regulation. However, its weaknesses often stemmed from its closed nature and lack of transparency. The 20th century's "new diplomacy" was born in reaction to the "old" (Weisbrode 2014, 13, 20). Diplomats were considered to be responsible for the war because they had failed to prevent World War I, and therefore, there was a strong reaction against "old diplomacy" and especially against secret diplomacy. It was argued that politics in the future would have to be shaped according to the needs of modern democracy and conducted under more "simple" rules than in the 18th and 19th centuries (Butterfield 1966, 181-182). Moreover,

historically, diplomacy had to adapt to technological developments and changes in economic, political, and social conditions. Railroads, steamships, and the electric telegraph created a communications revolution. This contributed to the definition of the trade and financial problems of industrializing societies' interns of policy objectives, and these problems were included in the field of diplomacy (Hamilton and Langhorne 2011, 93-94).

The new diplomacy was built on "public accountability" as a way to ensure that foreign policy depended on popular consent, on "self-determination" as a state-level extension of the liberal principle of individual rights, and on "collective security" as a mechanism to restrain the arbitrary use of force (Bjola and Kornprobst 2018, 53). The "new diplomacy" inspired by the Wilson Principles was, according to Weisbrode, in fact an interpretation of the views widely held in liberal circles in Britain, the United States, and Europe (Weisbrode 2024, 20).

The post-World War II fear of nuclear war did not put an end to states seeking changes to the status quo, but it did make states feel compelled to seek victories outside the use of force (Butterfield 1966, 190). An increasing number of industrial, social, and technological issues were considered to have an international and, therefore, diplomatic dimension. Moreover, the onset of the Cold War had the effect of reversing Carl von Clausewitz's famous maxim "war is the continuation of politics by other means." Diplomacy is often perceived as a form of warfare carried out by other means. Moreover, like the wars of the 20th century, diplomacy has become "total" both in its goals and in the issues it addresses (Hamilton and Langhorne 2011, 185). This transformation did not diminish the impact of the "new diplomacy" after 1945. It made itself and international politics more acceptable to popular and nominally democratic governments. By designing a communitarian, cooperative language, diplomacy preserved peace in Europe and reframed geopolitical problems as "functional" issues. This process reduced the tendency to use war as a foreign policy tool (Weisbrode 2014, 13, 20).

In the post-Cold War information age, technology-driven changes in the new diplomacy have occurred, and the need for diplomacy to adapt to the "digital world" has emerged. Improved capacity to collect and disseminate information has given policymakers and government institutions new opportunities to communicate their messages and set political agendas outside traditional channels in a world where everyone is increasingly connected. This transformation has been conceptualized as "digital diplomacy" or "DigiPlomacy". The development of e-mail, the use of websites by diplomatic missions and international organizations, and the proliferation of social media platforms such as Facebook, Twitter (X), and blogs are considered to be key components of digital diplomacy. It has been argued that the adoption of digital diplomacy has changed the way diplomats manage information, engage in public diplomacy, prepare strategies, participate in international negotiations, or even manage crises (Sharma 2023).

New technologies have the potential to facilitate complex diplomatic negotiations and redefine interactions between states and non-state actors (Frey 2024, 107-108). At this juncture, it is possible to say that convenient access to information and the increasing power of information have brought more actors – such as non-state armed actors – into diplomacy (Theander 2021, 2). In addition, technology and globalization have created a new imperative for us to be informed about everything that is happening all over the world. Diplomacy is no longer just about war and peace; it is about keeping track of enemies, rivals, competitors, allies, in short, everything that is happening all over the world (Pathak 2006, 52).

The worldwide adoption of digital platforms has brought with it a wave of openness and transparency that has never been experienced before (Rashica 2019, 23). The digital environment is a leaky place, and it is easier than ever to expose hostile and even peaceful government activity in real time (Wichowski 2015, 52). Indeed, the principle of secrecy in diplomacy is increasingly challenged by the easy dissemination of digital information to global audiences. Recent diplomatic leaks by activists such as Edward Snowden and Julian Assange have led to the perception that "the end of secrecy is near" in the postmodern digital age, where transparency is the order of the day (Bjola 2016, 2).

As a result, the expanding spheres of influence in diplomacy – the diversity of actors, the wave of openness/transparency, and the need for information analysis as a result of technological developments- have created the need for intelligence diplomacy. In the next section, the position of intelligence services in the changing understanding of diplomacy will be analyzed.

The Role of Intelligence Services as Foreign Policy Actors: Intelligence Diplomacy

Diplomacy and intelligence are the two main tools that every modern state, regardless of its political, military, and economic capacity, uses to achieve its foreign policy objectives and protect its national interests and security. Although the Ministries of Foreign Affairs and foreign intelligence services are two different institutions, their operational interests – collecting and analyzing information for foreign policy planning and managing relations with other actors – create a link between them (Markovski 2020, 18).

In the age of globalization, all nations must improve their information-gathering capabilities for both economic prosperity and security. They also have to assess the possibilities of information sharing for international security. This has led to a much closer partnership between diplomacy and intelligence, in terms of operational objectives (Pathak 2006, 51). Diplomacy and intelligence have been intertwined throughout history, and their juxtaposition is not new. However, technological advance has transformed intelligence from a limited "secret information gathering"

tool into a foreign policy instrument that performs a more strategic and proactive role. Communication between policymakers of states and other actors in world politics can also take place without the mediation of diplomats. For example, there is communication through direct meetings of political leaders of states and meetings of officials and intelligence personnel other than diplomats. This transformation took place in the 1960s, when it was believed that fast, direct communication in times of crisis was better than communication between groups specialized in diplomacy, such as the proliferation of "The Hotline" between heads of state (Bull 2002, 172).

As stand-alone institutions, intelligence services began to be part of 20th-century governments, and this association evolved over time, especially in foreign policy affairs. According to Herman, the difference from diplomacy is that intelligence provides information through special methods, while diplomacy uses it (Herman 1998, 1-22). Basically, on the surface, intelligence services gather information and foreign ministries use it to shape policy. Yet, in the background, diplomats also collect classified information.

Diplomacy has many functions, such as negotiation, representation, and communication. However, another purpose is to gather and disseminate information. None of the other functions can be effective without fulfilling this purpose. In other words, obtaining, sharing, and utilizing information for strategic purposes is the basis of diplomacy. States keep information such as designs of weapons, military operations, and diplomatic negotiation tactics secret from other actors. Most countries have official secrecy laws and complex rules on access to sensitive intelligence and national security information. Secrecy is a competitive, built-in aspect of dialogue between states. Illegally collecting information and sharing it with allies or the public has been controversial in all historical periods of diplomacy (Murray 2016, 13-15).

In the first half of the 18th century, Britain had a network of agents covering French and Spanish naval bases. In the same century, the spread of diplomacy led all European countries to seek to intercept and decode foreign diplomatic correspondence. However, intelligence services hardly existed during these centuries in the modern sense of permanent, professional institutions separate from diplomacy and foreign offices. Diplomats were expected to manage their own secret agents as part of their normal information gathering and political action. With the industrial revolution, the reflection of advanced technology on the battlefield produced new forms of warfare that required pre-planning based on information about the capacities of rival armies. This led to the creation of permanent and independent military intelligence departments. Initially, this did not affect the position of diplomacy. Embassies provided information on foreign forces through their military attachés. However, intelligence services grew in the early 20th century. The rate of technical and operational change in military capabilities has increased, and planned mobilization and deployment have increased the value of obtaining adversaries' plans. This made states more secretive about military matters (Herman 1998, 2-3).

In the Cold War period, intelligence and foreign policy became more intertwined as the struggle between the US and the Soviet Union took place in the gray zone due to the nuclear balance. Under the direction of the hegemonic actors of the era, covert operations conducted through foreign intelligence services served as a decisive foreign policy tool to protect national security interests. Covert operations as a means of achieving foreign policy objectives included covert activities such as propaganda, political operations, economic operations, coups, and the use of paramilitary proxies and intelligence services to influence each other's political, economic, military, and social conditions (Gök 2022a, 159-160).

The main objective of these actions is not to inform foreign policy decision-making, but to weaken or overthrow other governments by masking the involvement of the main actor. These activities involve international action, therefore, they obviously become a dimension of foreign policy. Notable examples include the Cold War-era funding of Italian anti-communist parties, the overthrow of governments in Iran and Guatemala, and the support of the Mujahideen in Afghanistan against Soviet forces (Munton 2018, 5).

In the post-Cold War era, advances in information technology brought a wave of openness and transparency in foreign policy, and it became easier than ever to simultaneously disclose secret government activities such as covert operations. This has transformed the relationship between foreign policy, diplomacy, and intelligence services.
Traditionally, while information from intelligence services supports the policy-making process, these services do not generally formulate foreign policy themselves (Munton 2018, 3). Moreover, according to this understanding, intelligence, unlike diplomacy, is not a decision-making and executive institution. In practice, there is often a clear distinction between intelligence and diplomatic professions (Herman 1998, 6).

However, in today's world, intelligence services play an active role in foreign policy-making processes. This new role transforms intelligence services themselves into structures that play a more active role in foreign policy decision-making processes, as opposed to classical intelligence service activities whose scope has long been limited to specific tasks (Darıcılı 2022). According to Mark Lowenthal, intelligence services can make four major contributions to policymaking: avoiding strategic surprises, providing long-term expertise, supporting the policy process, and protecting the confidentiality of information, needs, and methods (Lowenthal 2009).

While covert action and special operations have always existed, traditional diplomacy is being challenged by the expectation that modern-day organizations are increasingly "hunters, not gatherers." The WikiLeaks and Snowden incidents show that leaks of classified diplomatic communications can undermine the trust diplomats need to operate, especially where allies are concerned (Lomas 2021). The value of clandestine diplomacy processes involving intelligence services is that

they are more easily deniable, which is particularly important when the adversary is involved in armed attacks and/or terrorist activities. The role of intelligence services can be to support both national and international dialogue. The intelligence services are, indeed, very useful assets of the political will to engage in dialogue (Scott 2004, 331). With the growth of international cooperation, intelligence services operatives have become regular members of diplomatic missions in friendly and neutral countries, and intelligence has become a form of international diplomacy in its own right (Herman 1999, 203).

Recently, the concept of intelligence diplomacy has attracted growing interest in both academic and policy circles. However, there is not yet a generally accepted definition of the term. Some scholars narrowly define the concept as intelligence sharing with allies. Others see intelligence diplomacy as a more effective and broader form of public diplomacy. In general, intelligence diplomacy refers to the process by which foreign intelligence services are used to inform, encourage cooperation, enable joint actions, and deprive adversaries of strategic advantages. From the US perspective, intelligence diplomacy is used to "support the policies of policymakers in government, strengthen strategic relationships with foreign governments, and promote collective international action based on common interests." According to this perspective, an intelligence diplomacy process must meet three criteria: first, it must involve the public or direct sharing of objective intelligence with a foreign government; second, it should have the purpose of exchanging perspectives with a foreign government on a particular threat or problem; third, it should be done in support of advancing a preferred policy objective that may lead to unilateral, joint or multilateral action (Holmgren 2023).

Despite the diversity of definitions in the literature, this study situates intelligence diplomacy within a more specific and operational framework that extends beyond mere intelligence sharing. In this context, intelligence diplomacy is defined as the process whereby intelligence services, acting on behalf of the state, conduct negotiations, mediate, and engage in information sharing aimed at building trust in conflict environments where traditional diplomatic channels are deadlocked, political costs are high, or official contact carries significant risk. Although conflict resolution is a shared objective of both intelligence and diplomacy, the specific role of intelligence services in this domain has emerged as a distinct and critical area of inquiry. Accordingly, the following section examines this intersection in detail.

Intelligence Diplomacy in Conflict Resolution

While international conflict resolution is a field of study within the discipline of international relations, in terms of actors, it includes state institutions such as foreign ministries and intelligence services, political parties, international organizations, non-governmental organizations, universities, multinational corporations, and media (Gök 2022b, 241).

The aim of conflict resolution is not to avoid conflict, but rather to deal with it in a way that minimizes its inherent negative impact and maximizes its positive potential within the framework of peace values (Sanson and Bretherton 2001, 3). At this point, many different methods can be used together with actors at different levels to establish peace by developing solutions for the parties to the conflict. Today, as a result of the increase and spread of conflicts, different techniques have been forced to be developed for the resolution of conflicts and the search for the development and implementation of peaceful strategies to resolve conflicts through alternative methods involving soft power rather than hard power methods involving the use of force (Gök 2022b, 241).

Conflict resolution methods can generally be handled in four ways: (1) the use of force and coercive measures, (2) judicial and legal processes, (3) formal and informal bilateral methods, and (4) various forms of non-coercive, third-party interventions (which can be undertaken by a range of actors). These four ways of managing conflicts roughly correspond to power-based approaches to conflict (deterrence, sanctions), law-based approaches (invoking legal norms), and interest-based approaches (seeking common interests through bilateral negotiation and third-party mediation). Each approach has different features, characteristics, objectives, and outcomes; each requires different costs and resources, and each may be appropriate for different conflicts (Bercovitch and Gartner 2009, 4-5).

The use of intelligence diplomacy in conflict resolution falls within "interest-based approaches."
States make use of intelligence services as part of conflict resolution, and these actors go beyond gathering information about the parties to strengthen the ground for reconciliation and directly determine strategy as a foreign policy actor. The role of intelligence services in conflict resolution is, in fact, the essence of intelligence diplomacy, which, when used effectively, can provide a state with diplomatic leverage or political advantage.
The main types of activities that intelligence diplomacy involves in conflict resolution can be summarized as "secret negotiations, mediation, and information sharing."

Favored for centuries in resolving international disputes through diplomacy, confidential negotiations are an extremely common and functional method of conflict resolution in which officials of two or more actors discuss their disputes face-to-face. Negotiation is a cost-effective mechanism aimed at creating peace, creating a safe environment for peace to flourish, and ensuring sustainability through the application of justice (Meerts 2015, 21).

Negotiating institutions are successful when they are able to change or sustain the actions of a foreign government in a way that aligns their interests with those of the government they represent. During the communication process, those formulating policies will often revise their objectives in light of changing circumstances and

feedback from the foreign government. The communication process continues until consensus is reached or one government abandons or withdraws its demands (Galanton 2011, 100).

When seeking a solution to an armed conflict or political crisis, the parties involved often resort to secret negotiations. The aim is to avoid public awareness of the existence of negotiations at the outset. In some cases, both the process and its outcomes are intended to remain secret, and in other cases, the parties make the final results, on the whole or in part, public once the process has ended (IFIT 2019).

The most critical actors in secret negotiations, especially in conflicts involving non-state armed actors, are often intelligence services. When determining a negotiating strategy with groups such as terrorist organizations or national liberation movements, the most difficult decision is to strike a balance between secrecy and transparency. One of the main public objections to entering into negotiations is the risk of terrorist organizations legitimizing their aims and means. In such cases, negotiations can destabilize the political structures of the governments involved, hamper international efforts, and set a failed precedent (Neumann 2007, 128).
In order to overcome the obstacles encountered in such conflicts and to create a basis for negotiations, states prefer less visible but more effective intelligence diplomacy. This is because the covert nature and plausible deniability of intelligence activities make it possible to achieve similar foreign policy objectives with less public backlash.

There are many recent examples of secret negotiations between intelligence services and armed non-state actors. The most notable example is the US Central Intelligence Agency's (CIA) secret negotiations with the Taliban before the US military's complete withdrawal from Afghanistan in 2021.
William Burns, then CIA Director, a former diplomat, but who was considered the most experienced secret negotiator of the Joe Biden administration, held the highest-level face-to-face meeting to date on behalf of the US with Mullah Abdul Ghani Baradar, one of the Taliban leaders. It is stated that the negotiations sought a compromise on the US withdrawal process, the political and social situation in Afghanistan after the US withdrawal, and the fight against ISIS. The Taliban sees the Afghan branch of ISIS as a threat, and they are in conflict. At this point, the possibility of cooperation between the Taliban and the US on ISIS has emerged (BBC 2021). As a matter of fact, when the statements made by the US are analyzed, official sources frequently state that the most urgent threat in Afghanistan is ISIS and underline that the Taliban also has this idea (The New York Times 2021).

During the same period, a similar secret negotiation process with the Taliban was also conducted by the British Intelligence Service MI6. According to Miller, "The secret talks between the Taliban and MI6 during the evacuation of Kabul represent the final chapter in the British Intelligence Service's longstanding engagement with radical Islamist groups in Afghanistan" (Miller 2021). The strategy of negotiation that

began during the Cold War to break the Soviet sphere of influence continued in 2007 when MI6 agents held talks with Taliban members in Afghanistan to persuade them to stop fighting against the Afghan government (Politics.co.uk 2007). In the recent past, however, senior British intelligence officials held secret talks with the Taliban in Kabul to obtain assurances that Afghanistan would not be used for terrorist attacks against the West (The Telegraph 2021).

There are noteworthy examples in the recent past of negotiation processes carried out within the framework of intelligence diplomacy between states, with important implications for conflict resolution.
In 2020, Yossi Cohen, then head of the Mossad, negotiated the normalization of relations between the United Arab Emirates (UAE) and Israel, which is an important example of intelligence diplomacy. As a result of Cohen's secret negotiations throughout 2020, the UAE officially declared its recognition of Israel on August 13, 2020, and this process was formalized with the "Abraham Accords" signed at the White House on September 15, 2020 (Reuters 2020).

It has a historical significance in that the Arabs, who have long been at odds with Israel over the Palestinian issue, wanted to shift the intra-regional balance of power in their favor due to the growing Iranian threat in the region and took steps of mutual cooperation with Israel in this direction (Yaman and Yiğittepe 2023). In this context, apart from normalizing relations between Israel and the UAE and Israel and Bahrain, geopolitically, the agreements were expected to strengthen the informal anti-Iran alliance in the region, increase pressure on Tehran, and strengthen US ties with key allies in the Middle East (Norlen and Sinai 2020).
A similar example of intelligence diplomacy was seen in the initiatives that paved the way for the normalization process between Türkiye and Egypt in 2023. Hakan Fidan, then the head of the National Intelligence Service of Türkiye (MIT), was involved in secret negotiations for the normalization of Türkiye's bilateral relations with Egypt (Hurriyetdailynews 2023).

Türkiye's improved relations with Egypt can be considered as one of the most important steps in the regional normalization process. The policies pursued by the two countries, which adopted different and even confrontational attitudes towards each other on the basis of discourse in regional crises such as Libya and the Eastern Mediterranean, started to harm their regional interests (Ataman 2023). As a matter of fact, these negotiations were conducted with the aim of providing geopolitical and geostrategic benefits to the two countries in the Eastern Mediterranean, as well as being the product of a common interest-based approach.

Another important activity of intelligence diplomacy in conflict resolution is mediation. International conflicts are becoming increasingly complex and pose a threat to global peace and security. In this context, mediation gains key importance as a mechanism to prevent violence and find a peaceful solution. Mediation is a process of intervention by a neutral third party that helps conflict parties to reach

a common understanding and agreement through dialogue and negotiation. This process aims to create an environment of trust where conflicting parties can express their interests and concerns and seek mutually satisfactory compromise options. One of the attractive functions of mediation in international relations is that it can be applied to different types of conflicts and actors. It can be applied to territorial disputes, economic disputes, national identities, and broader contexts such as religious or ethnic conflicts. It is important to emphasize that mediation not only contributes to ending hostilities but also helps to build the foundations for long-term peace and cooperation (Zhomartkyzy 2023, 169-170).

The mediation process is methodological as well as theoretical and needs to be addressed through expert knowledge, sophisticated analysis, and intelligence (Nathan 2014, 225). This is why intelligence services in particular are playing an increasingly important role in mediation processes.
This is because existing mediation approaches and their results have become inadequate over time due to changes in mediation motivations, actors' intentions, and the nature of conflicts. As a result, there have been changes in the nature of mediation with new approaches both in literature and in practice (Kiraz 2020, 230). Because interstate competition has taken on a hybrid character in the gray zone and the element of "plausible deniability" has increased in this process, the mediating ability and scope of traditional diplomacy have been limited.

Similar criticism was made in the summary report of the Fourth Istanbul Mediation Conference, which discussed the development of mediation within the UN. According to the report, although international organizations have played an increasing role in the early stages of conflict and post-conflict phases in the post-Cold War era, their involvement in post-conflict reconstruction is declining. In this respect, there are fewer diplomats but more military and intelligence personnel on the ground today. Therefore, in recent times, conflict resolution has been predominantly focused on intelligence diplomacy: a country can mediate to establish peace in another country through its intelligence services (Herman 1999, 156).

While there are many current examples of mediation involving intelligence services, Türkiye has become one of the actors contributing to the institutional development of mediation by giving importance to mediation activities in its foreign policy since 2010 (Kiraz 2020, 228). In this context, it is seen that MIT has carried out effective mediation activities in conflicts and crises through intelligence diplomacy. MIT has carried out important activities in intelligence diplomacy, such as the exchange of 200 prisoners of war between Russia and Ukraine in 2022, the intelligence contacts between the US and Russia, and the coordination of the prisoner exchange between the two countries (Şahin 2022). The most high-profile of these activities was the most comprehensive prisoner swap between Russia and the US since the Cold War, which took place in Ankara on August 1, 2024, with the mediation of MIT (Seren 2024).

With the organization of MIT, the parties were brought together in Türkiye in July 2024. The swap between citizens of Western countries and Russian citizens

imprisoned in the US, Germany, Poland, Norway, Slovenia, Russia, and Belarus was mediated (Hürriyet Gazetesi 2024). In the operation in which a total of 26 prisoners were exchanged, 10 people detained in the US and other Western countries were released, while Russia handed over 16 prisoners to the US (Seren 2024).

Another recent mediation activity of MIT was between Israel and Hamas after October 7. MIT played an important role in this process, conducting intensive diplomacy with Hamas senior leadership, Israel, Egypt, Qatar, and the US, and mediating between Israel and Palestine on issues such as ceasefire and prisoner exchange. In the context of requests for assistance from foreign countries, MIT mediated the release of some foreign hostages in Gaza and helped Hamas release 5 Thai hostages on January 30, 2025 (Şimşek 2025).

Consequently, when direct negotiations between the parties are not possible, intelligence services as intermediary actors can be involved in conflict resolution not only as information gatherers or analysts, but also as actors managing the technical and strategic components of mediation.
Although intelligence services have become the guiding and decision-making actors in conflict resolution processes, they continue to use the power of information as a tool in intelligence diplomacy. Indeed, information sharing for cooperation in intelligence diplomacy plays a critical role in building trust between the parties and sustaining communication channels.

International intelligence cooperation is the liaison between relevant actors responsible for the collection, analysis, and/or dissemination of intelligence for purposes such as defense, national security, and the prevention and detection of transnational crime, and information sharing is an important step in this process (Born, Leigh and Wills 2015, 15).

Intelligence services tend to protect information because they fear that sharing it could result in disclosure, which could reveal important sources and methods and threaten the organization's ability to collect intelligence in the future (Roach 2012, 131). Since the end of the Cold War, threats have become increasingly transnational in nature. The acceleration of globalization has contributed to the expansion of the scope and pervasiveness of networks engaged in activities such as organized crime, proliferation of weapons of mass destruction, and terrorism. The growth of these transnational threats has forced intelligence services to cooperate with their counterparts in other states to meet these challenges. Although cooperation in certain areas of intelligence operations (e.g., signals intelligence) has been longstanding, particularly among Western states, there has been an increase in both the scope and scale of intelligence cooperation since 9/11 (Leigh 2011, 3).

Intelligence cooperation is also an extension of foreign policy. In many states, intelligence services are very close to the executive, and their work is closely aligned with the priorities of the incumbent government. Generally speaking, intelligence

cooperation will be followed by a state's foreign relations (Born, Leigh and Wills 2015, 17-18).

Shared intelligence is valuable if it sheds light on important foreign policy issues. Recipient states wish to make sure that their partners provide accurate information and analysis-based intelligence that complements their own efforts. Such information, which cannot otherwise be obtained at a reasonable cost, can be useful even if it does not directly lead to changes in foreign policy. For example, shared intelligence can increase confidence in the information held by the receiving state by corroborating existing information. This, in turn, confirms the accuracy of current policy and can reduce the pressure to change strategy (Walsh 2007, 157).

Intelligence components are often difficult to implement, especially in multinational peacekeeping operations. Tactical and strategic cooperation for successful conflict resolution has therefore been limited. As the international community has demanded better and more effective use of peacekeeping forces, a sense of insecurity created by national interests has tightly controlled intelligence cooperation in multinational interventions (Larsson 2010). In such operations, intelligence gathering was mainly undertaken by the intelligence services of the cooperating states (Díaz 2007, 33). On the other hand, the sense of insecurity created by hybrid threats has forced international cooperation mechanisms to be more flexible, especially in terms of intelligence sharing. For example, NATO has reformed its intelligence institutions to facilitate support to member states' foreign policy decision-making and operations, including enhanced warning systems and intelligence sharing against hybrid threats. With the establishment of the Joint Intelligence and Security Division (JISD) in 2017, the Alliance began to unify intelligence sharing to counter hybrid threats and joint operations (Gök 2024). NATO's intelligence-sharing reform was put to the test during Russia's intervention in Ukraine in 2022.

In the fall of 2021, US intelligence had strong indications that Russia was preparing to invade Ukraine, and President Biden sent then CIA Director Bill Burns to Russia to conduct intelligence diplomacy. The aim was to make Russia back down by making it feel that its plans were known. However, these contacts did not yield any concrete results. The US then decided to share information with its allies, which was subsequently leaked to the press. This put Russia's military preparations on the agenda of the international community. In January, the US discovered that Russia was planning a fake attack and made it public, thus frustrating the disinformation attempt (Calabresi 2024).

Ultimately, the essence of intelligence diplomacy rests on the growing awareness among relevant actors that information is a strategic asset that, when used wisely, can provide diplomatic leverage. Indeed, the US proactive sharing of intelligence regarding Russian intentions and mobilization with NATO allies prior to the 2022 invasion of Ukraine not only established a strategic narrative of aggression but also enabled the international community to recognize the true nature of the intervention as it unfolded. Moreover, thanks to this sharing, hybrid warfare strategies such

as "false flag operations", which the Russians successfully employed in the 2014 annexation of Crimea, were ineffective in the 2022 intervention (Shapiro 2024).

The incident clearly demonstrated the utility of intelligence diplomacy as a tool for influence, both in terms of negotiation and information sharing. By effectively using intelligence diplomacy to guide its allies, prepare the international community, and break the psychological superiority of its rival, Russia, the US has added a new dimension to its conflict resolution approaches, even though the conflict in Ukraine continues today.

In conflict resolution, intelligence diplomacy enables information sharing between actors, effective cooperation and swift adaptation to changing priorities and contexts, and efficient resource allocation. Information also enhances situational awareness. Conversely, conflicts may escalate in the absence of such information. The importance and challenges of intelligence sharing in multinational peacekeeping operations were particularly evident in the international community's intervention in Mali following the 2012 uprising by armed separatists against government forces in northern the country. The French-led military intervention that began in early 2013 prevented anti-government forces from advancing further south, and, in the same year, a peacekeeping force was deployed to Mali under United Nations Security Council Resolution 2100 to restore stability in the country. After a decade of operations, a deteriorating security situation, and other setbacks in 2020 and 2021, the French military force withdrew amid deepening distrust of the Malian government's actions and intentions. Subsequently, the UN mission suspended its activities and withdrew its personnel in 2023 after Malian authorities demanded its departure (Sims 2024; Fabra 2022).

The lack of a centralized, trust-based information-sharing system among the actors involved in the Mali mission hindered communication and coordination, ultimately undermining operational effectiveness and leading to mission failure (Sims 2024). Concurrently, a series of political miscalculations, such as the obstruction of negotiation initiatives and the prioritization of broader stability over accountable governance, played a significant role. France's engagement in the Sahel was predicated almost entirely on a military-centric strategy, failing to address the root causes of the conflict. This situation was further exacerbated by operational failures, particularly the collaboration with armed groups, which undermined local state authority and inflamed ethnic tensions (Powell 2022). The French General Directorate for External Security (DGSE) also faced scrutiny for its inability to anticipate these developments, largely attributed to a paucity of reliable human intelligence (HUMINT) assets on the ground. Given that coup preparations were conducted by tightly knit, compartmentalized groups, infiltrating such formations proved exceptionally challenging for foreign entities. This reality underscored the vital importance of intelligence diplomacy and deeper collaboration with local counterparts (Aksan 2023).

The Mali example demonstrates that the capacity to overcome information challenges stemming from uncertainty and complexity is essential for supporting the tactical

and operational levels of peacekeeping missions. Conversely, at the strategic level, it is crucial that information analysts mitigate uncertainty and ambiguity through effective information sharing to clarify the decision-making context (Duursma 2018, 465). In this context, intelligence diplomacy assumes a pivotal role. For peacekeeping missions to succeed, establishing a comprehensive and trust-based diplomatic framework among stakeholders is imperative.

Conclusion

The multiple case analysis conducted in this study reveals that the success of intelligence diplomacy is driven not only by case-specific (idiosyncratic) local dynamics, but also by structural transformations within the international system. The hybridization of the security environment and the proliferation of non-state actors in the post-9/11 era have elevated intelligence services from an auxiliary instrument of foreign policy to a primary diplomatic actor. The findings of the study demonstrate that, challenging the limited conceptualization in the existing literature, intelligence diplomacy plays a constitutive rather than a complementary role in gray zones where formal diplomacy has reached an impasse. The case analysis highlights the fact that the efficacy of intelligence diplomacy is most pronounced in three key activities: covert negotiations, mediation, and information sharing. In regions where state authority is weakened, such as the Middle East, the Sahel, and Eastern Europe (Ukraine), the adaptive nature of intelligence services provides states with significant operational latitude. From back-channel negotiations with the Taliban to prisoner exchanges in the Russia-Ukraine War, numerous examples demonstrate that intelligence diplomacy has evolved from a mere technical instrument of crisis management into a strategic imperative.

Consequently, intelligence diplomacy is no longer a transient expedient for crisis management but an integral element of modern statecraft. However, this expanded mandate inevitably introduces significant legal and normative challenges. Looking forward, intelligence services are expected to evolve into hybrid institutions that not only gather operational data but also monitor ceasefire regimes on the ground and provide solution-oriented analytical frameworks. To ensure the viability of this transformation, it is imperative to establish robust democratic oversight mechanisms, preserve the equilibrium between institutional autonomy and foreign policy objectives, and mitigate operational risks.

References

Aksan, S. 2023. "Fransız istihbaratı Nijer'de sınıfta mı kaldı?" *TRT Haber*. https://www.trthaber.com/haber/gundem/fransiz-istihbarati-nijerde-sinifta-mi-kaldi-787514.html.

Ataman, M. 2023. "Normalleşme Sürecinin Son Cephesi: Türkiye-Mısır İlişkilerinin Gelişmesi." *Kriter* 7 (78). https://kriterdergi.com/dis-politika/normallesme-surecinin-son-cephesi-turkiye-misir-iliskilerinin-gelismesi.

Athanasiadis, I. 2024. "With Israel, Palestine and Lebanon on Fire, Why is UN Mediation Absent?" *Stimson*. https://www.stimson.org/2024/with-israel-palestine-and-lebanon-on-fire-why-is-un-mediation-absent/.

BBC. 2021. "Afghanistan: Secret Kabul talks between CIA and Taliban - US media." https://www.bbc.com/news/world-asia-58320516.

Bercovitch, J., and S. S. Gartner. 2009. "New Approaches, Methods and Findings in the Study of Mediation." In *International Conflict Mediation: New Approaches and Findings*, edited by J. Bercovitch and S. S. Gartner, 1–42. New York: Routledge.

Bjola, C. 2016. "Introduction: The Theory and Practice of Secret Diplomacy." In *Secret Diplomacy: Concepts, Contexts and Cases*, edited by C. Bjola and S. Murray, 1-9. New York: Routledge.

Bjola, C., and M. Kornprobst. 2018. *Understanding International Diplomacy: Theory, Practice and Ethics*. New York: Routledge.

Born, H., I. Leigh, and A. Wills. 2015. *Making International Intelligence Cooperation Accountable*. Printing Office of the Parliament of Norway. https://www.dcaf.ch/sites/default/files/publications/documents/MIICA_book-FINAL.pdf.

Bull, H. 2002. *The Anarchical Society: A Study of Order in World Politics*. New York: Palgrave.

Butterfield, H. 1966. "The New Diplomacy and Historical Diplomacy." In *Diplomatic Investigations*, edited by H. Butterfield and M. Wight, 181-192. Cambridge: Harvard University Press.

Calabresi, M. 2024. "Inside the White House Program to Share America's Secrets." *Time*. https://time.com/6835724/americas-intelligence-secrets/.

Darıcılı, A. B. 2022. "How Intelligence Agencies Turned into Foreign Policy Tools." *Politics Today*. https://politicstoday.org/intelligence-agencies-as-foreign-policy-tools/.

Debo, D. 2023. *The Role of Information and Intelligence in Foreign Policy Decision-Making*. LVR Center-Libra Academy.

Díaz, G. 2007. "Intelligence at the United Nations for Peace Operations." *UNISCI Discussion Papers* 13. https://www.ucm.es/data/cont/media/www/pag-72528/Gustavo13a.pdf.

Duursma, A. 2018. "Information Processing Challenges in Peacekeeping Operations: A Case Study on Peacekeeping Information Collection Efforts in Mali." *International Peacekeeping* 25 (3): 446-468. https://doi.org/10.1080/13533312.2018.1446757.

Fabra, J. B. 2022. "Analysis of the United Nations Peace Operation in Mali: Counterterrorism and Counterinsurgency in MINUSMA." *Revista Análisis Jurídico-Político* 4 (8): 17-50. https://doi.org/10.22490/26655489.5845.

Frey, C. 2024. "Digital Diplomacy: The Impact of Technology on Modern Diplomacy and Foreign Policy Current Realities and Future Prospects." *Romanian Journal of European Affairs* 24 (1): 107-126. https://rjea.ier.gov.ro/wp-content/uploads/2024/06/Art.-5_Digital-diplomacy_Frey_2024_final.pdf.

Galanton, D. 2011. "The Diplomatic Negotiation – A Key Factor In International Relations." *Outlook on Communication* 1 (2): 100-108. https://ijcr.eu/articole/22_pdfsam_IJCR%202-2011.pdf.

Gök, A. 2022a. "Örtülü Operasyonlar ve Faaliyetler." In İstihbarat Çalışmaları, edited by C. K. Demir and S. Yenal, 159-184. Ankara: Nobel Yayınları.

___. 2022b. "Uluslararası Çatışma Çözümünde Kamu Diplomasisinin Rolü." In *Uluslararası Çatışma Çözümü Hukuksal Yöntemlerden Alternatif Çatışma Çözümüne*, edited by Muzaffer Ercan Yılmaz, 241–56. Ankara: Nobel Yayınları.

___. 2024. "İstihbarat ve Güvenlik: Değişen Güvenlik Algısında NATO'nun İstihbarat Kurumları." In *Güvenliği Yeniden Okumak: Güvenlik Çalışmalarında Kavramlar, Aktörler ve Güncel Konular*, edited by H. Arıkan and A. Gök, 277-295. Ankara: Yetkin Yayınları.

Hamilton, K., and R. Langhorne. 2011. *The Practice of Diplomacy*. New York: Routledge.

Herman, M. 1998. "Diplomacy and Intelligence." *Diplomacy and Statecraft* 9 (2): 1-22.

___. 1999. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Holmgren, B. M. 2023. "Intelligence and Diplomacy: A New Model for a New Era." *U.S. Department of State*. https://2021-2025.state.gov/intelligence-and-diplomacy-a-new-model-for-a-new-era/.

Hurriyet Daily News. 2023. "Turkish, Egyptian top diplomats discuss normalization road map." https://www.hurriyetdailynews.com/turkish-egyptian-top-diplomats-discuss-normalization-road-map-183872.

Hürriyet Gazetesi. 2024. "MİT koordine etti: Ankara'da ABD ile Rusya arasında esir takası." https://www.hurriyet.com.tr/gundem/mit-koordine-ediyor-ankarada-abd-ile-rusya-arasinda-esir-takasi-42497738.

IFIT (Institute for Integrated Transitions). 2019. *Process Design for Secret Negotiations*. IFIT Practice Brief. https://ifit-transitions.org/wp-content/uploads/2021/03/Process-Design-for-Secret-Negotiations.pdf.

Kiraz, S. 2020. "Uluslararası Arabuluculuğa Dair Değişen Yaklaşımlar ve Türkiye'nin Arabuluculuğun Dönüşümündeki Rolünün İncelenmesi." *Akdeniz İİBF Dergisi* 20 (2): 227-238. https://doi.org/10.25294/auiibfd.827500.

Larsson, P. 2010. "The United Nations, Intelligence and Peacekeeping: International Relations at Play." Bachelor's thesis, Lund University. https://lup.lub.lu.se/student-papers/search/publication/1567364.

Leigh, I. 2011. "Accountability and Intelligence Cooperation: Framing the Issue." In *International Intelligence Cooperation and Accountability*, edited by H. Born, I. Leigh, and A. Wills, 3-17. New York: Routledge.

Lomas, D. W. B. 2021. "Intelligence and Diplomacy: Changing Environment, Old Problems." *Salford University Repository*. https://salford-repository.worktribe.com/OutputFile/1488030.

Lowenthal, M. M. 2009. *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press.

Markovski, D. 2020. "Diplomacy and Intelligence Services: Reflection on Small States." *International Scientific Journal on European Perspectives* 11 (1): 17-39. https://www.europeanperspectives.org/storage/105/03-International-Scientific-Journal-on-European-Perspectives-December-2020-DIPLOMACY.pdf.

Meerts, P. 2015. *Diplomatic Negotiation: Essence and Evolution*. Clingendael Institute. https://www.clingendael.org/sites/default/files/pdfs/Diplomatic_Negotiation_Web_2015.pdf.

Miller, P. 2021. "How MI6 backed 'right-wing religious fanatics' in Afghanistan." *Declassified UK*. https://www.declassifieduk.org/how-mi6-backed-right-wing-religious-fanatics-in-afghanistan/.

Morgenthau, H. J. 1948. *Politics among Nations: The Struggle for Power and Peace*. New York: Alfred A. Knopf.

Munton, D. 2018. "Diplomacy and Intelligence." In *The Encyclopedia of Diplomacy*, edited by G. Martel. John Wiley and Sons. https://doi.org/10.1002/9781118885154.dipl0077.

Murray, S. 2016. "Secret 'versus' Open Diplomacy across the Ages." In *Secret Diplomacy: Concepts, Contexts and Cases*, edited by C. Bjola and S. Murray, 13-29. New York: Routledge.

Nathan, L. 2014. "The Intelligence Requirement of International Mediation." *Intelligence and National Security* 29 (2): 208-226. https://doi.org/10.1080/02684527.2013.799368.

Neumann, P. R. 2007. "Negotiating with Terrorists." *Foreign Affairs* 86 (1): 128-138.

Norlen, T., and T. Sinai. 2020. "The Abraham Accords: Paradigm Shift or Realpolitik?" *Security Insights*, no. 64. https://www.marshallcenter.org/sites/default/files/files/2020-10/Security%20Insights%2064%20-%20Norlen%20SInai%20-%20The%20Abraham%20Accords%20-%20OCT%202020.pdf.

Pathak, D. C. 2006. "Diplomacy and Intelligences." *Indian Foreign Affairs Journal* 1 (2): 47-57. https://www.jstor.org/stable/45340560.

Politics.co.uk. 2007. "Taliban and MI6 in talks." https://www.politics.co.uk/news/2007/12/26/taliban-and-mi6-in-talks/.

Powell, N. 2022. "Why France Failed in Mali." *War on the Rocks.* https://warontherocks.com/2022/02/why-france-failed-in-mali/.

Rashica, V. 2019. "Digital Diplomacy: Aspects, Approaches and Practical Use." *International Scientific Journal on European Perspectives* 1 (7): 21-39. https://www.europeanperspectives.org/storage/24/DIGITAL-DIPLOMACY_Rashica.pdf.

Reuters. 2020. "Mossad head meets UAE national security adviser: WAM agency." https://www.reuters.com/article/world/mossad-head-meets-uae-national-security-adviser-wam-agency-idUSKCN25E1UT/.

Roach, K. 2012. "Overseeing Information Sharing." In *Overseeing Intelligence Services: A Toolkit*, edited by H. Born and A. Wills, 129-147. Geneva: DCAF.

Sanson, A., and D. Bretherton. 2001. "Conflict Resolution: Theoretical and Practical Issues." In *Peace, Conflict, and Violence: Peace Psychology for the 21st Century*, edited by D. J. Christie, R. V. Wagner, and D. A. Winter. New Jersey: Prentice-Hall.

Scott, L. 2004. "Secret Intelligence, Covert Action and Clandestine Diplomacy." *Intelligence and National Security* 19 (2): 322-341. https://doi.org/10.1080/0268452042000302029.

Seren, M. 2024. "Esir takası operasyonu: MİT istihbarat diplomasisinde ağırlığını ortaya koydu." *Anadolu Ajansı*. https://www.aa.com.tr/tr/analiz/esir-takasi-operasyonu-mit-istihbarat-diplomasisinde-agirligini-ortaya-koydu/3293496.

Şahin, S. 2022. "MİT etkin istihbarat diplomasisi ile küresel krizlerde çözüme kapı araladı." *Anadolu Ajansı*. https://www.aa.com.tr/tr/gundem/mit-etkin-istihbarat-diplomasisi-ile-kuresel-krizlerde-cozume-kapi-araladi/2776090.

Shapiro, J. 2024. "Letter from Washington: All-knowing America and US intelligence diplomacy." *European Council on Foreign Relations*. https://ecfr.eu/article/letter-from-washington-all-knowing-america-and-us-intelligence-diplomacy/.

Sharma, N. 2023. "Digital Diplomacy: The Evolution of a New Era in Diplomacy." *RIS*. https://ris.org.in/sites/default/files/2023-01/interns/topics/Nandika-Sharma.pdf.

Şimşek, U. 2025. "MİT, Hamas'ın elindeki 5 Taylandlı rehinenin Gazze'de serbest bırakılmasını sağladı." *Anadolu Ajansı*. https://www.aa.com.tr/tr/gundem/mit-hamasin-elindeki-5-taylandli-rehinenin-gazzede-serbest-birakilmasini-sagladi/3466899.

Sims, C. 2024. "Information Sharing and the Effectiveness of Peacekeeping Operations in Mali." *Military Review*. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/September-October-2024/Information-Sharing/Information-Sharing-UA.pdf.

Theander, F. 2021. "Digital Diplomacy: A Study of Social Media and the Changing Role of the Diplomatic Service." Master's thesis, Lund University.

The New York Times. 2021. "Amid Afghan Chaos, a C.I.A. Mission That Will Persist for Years." https://www.nytimes.com/2021/08/27/us/politics/cia-afghanistan.html.

The Telegraph. 2021. "MI6 holds talks with Taliban to prevent terrorists plotting attacks from Afghanistan." https://www.telegraph.co.uk/news/2021/08/31/mi6-holds-talks-taliban-prevent-terrorists-plotting-attacks/.

Walsh, J. I. 2007. "Defection and Hierarchy in International Intelligence Sharing." *Journal of Public Policy* 27 (2): 151-181. https://www.jamesigoewalsh.com/jpp2007.pdf.

Weisbrode, K. 2014. *Old Diplomacy Revisited*. New York: Palgrave.

Wichowski, A. 2015. "'Secrecy is for losers': Why diplomats should embrace openness to protect national security." In *Digital Diplomacy: Theory and Practice*, edited by C. Bjola and M. Holmes, 52-70. New York: Routledge.

Wight, M. 1978. *Power Politics*. New York: Holmes and Meier.

Yaman, D., and L. Yiğittepe. 2023. "Israel Gulf Expansion Within Regional Security Complex Theory: The Effect Of The Abraham Accords On The Power Balances in The Region." *Karamanoğlu Mehmetbey Üniversitesi Sosyal ve Ekonomik Araştırmalar Dergisi* 25 (45): 879-901. https://izlik.org/JA23SC88GC.

Zhomartkyzy, M. 2023. "The Role of Mediation In International Conflict Resolution." *Law and Safety* 90 (3): 169-178. https://doi.org/10.32631/pb.2023.3.14.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Artificial Intelligence as a Geostrategic Vector in Reshaping the 21st Century Balance of Power

Dipl. Eng. Dumitru-Cătălin VASILE, EMBA, Ph.D. Candidate*

*National University of Political Studies and Public Administration, Bucharest, Romania
"Carol I" National Defense University, Bucharest, Romania
"Mihai Viteazul" National Intelligence Academy, Bucharest, Romania
e-mail: catalin.vasile@outlook.com
https://orcid.org/0009-0003-3257-4156

Abstract

Artificial Intelligence (AI) has moved beyond its status as an emerging technology to become the primary vector of geostrategic competition in the 21st century. This paper argues that AI is not merely a tool but a new domain of confrontation that fundamentally reshapes the metrics of national power. The original contribution of this article lies in identifying and analyzing the critical asymmetry between the components of digital power. While data and talent are diffusing resources, computing power (hardware) represents a "choke point" that dictates the global hierarchy. By analyzing the competition between the United States and China, the work examines how the race for AI supremacy redefines military doctrines and economic alliances. In addition, the study specifies the impact of this competition on NATO's Eastern Flank, demonstrating that for states like Romania, the transition toward algorithmic security is not optional but a survival imperative in the face of hybrid warfare. The paper is structured into four chapters covering the foundations of power, military implications, the "Technological Cold War," and global ideological divergence.

Keywords:

Artificial Intelligence (AI); Geostrategy; Balance of Power; US-China Competition; Technological Cold War; International Security; Algorithmic Warfare, AI Governance; Semiconductors.

Article info
Received: 16 November 2025; Revised: 18 December 2025; Accepted: 22 February 2026; Available online: 8 April 2026

Citation: Vasile, D.C. 2026. "Artificial Intelligence as a Geostrategic Vector in Reshaping the 21st Century Balance of Power." *Bulletin of "Carol I" National Defence University*, 15(1): 77-86. https://doi.org/10.53477/2284-9378-26-05

Introduction

The history of international relations is essentially the history of how disruptive technologies have reconfigured power. From the longbow to the steam engine and, eventually, the nuclear weapon, those who mastered the defining technology of an era dictated the terms of the global order. Today, we are at a similar inflexion point. AI represents a revolution of a magnitude that many analysts believe exceeds that of the nuclear revolution. This competition aligns perfectly with the realist school of international relations, which posits that states are in a perpetual struggle for power and security within an anarchic system. AI becomes the latest and possibly most powerful weapon in this zero-sum game. Kissinger, Schmidt, and Huttenlocher (2021) capture this transformation, stating that AI is more than a simple innovation; it challenges the very foundations of human thought and strategic order.

> "What lies ahead of us is a potentially even more radical transformation of human consciousness and the human condition... Artificial Intelligence is poised to transform all fields of human experience. Moreover, its strategic implications, which stem from this transformation, are monumental." (Kissinger, Schmidt and Huttenlocher 2021, 14)

The geostrategic stakes are perceived at the highest level. In a famous 2017 statement, Russian President Vladimir Putin summarized the competition in clear terms: "Artificial Intelligence is the future, not only for Russia but for all of mankind... Whoever becomes the leader in this sphere will become the ruler of the world" (quoted in Associated Press 2017).

Unlike nuclear weapons, which are expensive, difficult to develop, and have as their primary utility their non-use (deterrence), AI is inexpensive, rapidly disseminated, and possesses an intrinsic dual nature (civilian and military). It is not just a weapon; it is a force multiplier that simultaneously affects the economy, surveillance, propaganda, logistics, and military command. This paper analyzes how AI functions as a geostrategic vector, becoming the epicenter of the "Great Competition" between the United States and China, a dynamic that evokes "Thucydides' Trap" (Allison 2017). The central argument is that the nation that achieves AI supremacy will gain a decisive advantage in shaping the balance of power in the 21st century.

While the existing literature abounds with analyses of the economic impact of AI or the broader US-China competition, this paper makes a distinct scientific contribution by shifting the focus from capabilities to structural vulnerabilities. Unlike approaches that treat AI as a technological monolith, this analysis deconstructs the triad of power (data-algorithms-hardware) to demonstrate that hardware (advanced semiconductors) represents the determinant independent variable of the new world order. Furthermore, the paper extends the theoretical framework beyond the great powers, proposing a necessary analysis of the implications for frontier states (such as Romania) through the lens of algorithmic security.

1. New foundations of national power in the algorithmic era

Traditionally, geostrategic power was evaluated by GDP, population size, military strength, and natural resources. The AI era introduces a new triad of power: data, talent (human capital), and computing power (semiconductors).

1.1. Data as a strategic resource – "The New Oil."

If oil-based economies dominated the 20th century, the 21st century is dominated by data-based economies, necessary for training deep learning models. China's structural advantage, theorized by Kai-Fu Lee (2018), lies in massive access to data through a centralized state model, which led him to state that 'if data is the new oil, then China is the new Saudi Arabia' (Lee 2018, 18). This immense volume of data allows for the training of more precise algorithms for everything from facial recognition to commercial logistics.

However, the analogy with oil has its limits. Unlike oil, which is a finite resource, data is generative (its use creates even more data), and its value increases when combined. Moreover, it is not just the quantity of data that is important, but also its quality and diversity. Here, the Western ecosystem might hold a long-term advantage: data coming from open and diverse societies could be more valuable for training robust algorithms capable of handling unforeseen scenarios

1.2. The War for talent and innovation ecosystems

AI is a field where a single top-tier researcher can have a disproportionate impact. The competition to attract and retain AI talent is fierce. While the US benefits from elite universities and the draw of Silicon Valley, China utilizes aggressive talent repatriation programs (Allen 2019).

This competition is complicated by the fact that most top talent does not work for governments but for a very small number of private corporations. Amy Webb (2019) argues in The Big Nine that the future of AI is controlled by nine giants, six American and three Chinese. This creates a fundamental geostrategic tension: while nation-states (the US and China) are in strategic competition, the critical resources that top researchers control are controlled by corporations whose goals, such as global profit, are not always in sync with national security interests.

1.3. Computing power – hardware as a Choke Point

Algorithms and data are useless without the specialized hardware (primarily GPUs) required to process them. This dependency creates critical geostrategic choke points. Sovereignty in the 21st century means "digital sovereignty" and "chip sovereignty" (Miller 2022).

This choke point is extremely specific and fragile. The entire global AI ecosystem depends on a single technology for producing the most advanced chips (under 7nm): Extreme Ultraviolet (EUV) lithography. This technology is monopolized by a single company worldwide, ASML (Netherlands). Export control of this specific technology represents the West's most powerful geostrategic weapon.

Miller (2022) argues that the battle for control of this supply chain, which stretches from the Netherlands to Taiwan (TSMC) and South Korea (Samsung), is more important than traditional military battles.

The contribution of this analysis to the specialized literature lies in identifying a critical asymmetry among the components of the triad: while data and talent are diffuse resources, computing power is a finite, geographically constrained, and technologically specific choke point. Unlike analyses that treat the three elements as equally important, this paper argues that hardware is the only absolute barrier that can create an insurmountable gap between global powers in the current decade.

2. The AI-based Revolution in Military Affairs (RMA)

AI is not just changing the tools of war, but its very nature. We are witnessing a Revolution in Military Affairs (RMA) as profound as the introduction of the tank or aviation.

2.1. Algorithmic warfare and Lethal Autonomous Weapons Systems (LAWS)

AI enables the development of Lethal Autonomous Weapons Systems (LAWS), which can select and attack targets without direct human intervention. This radically compresses the "OODA loop" (Observation, Orientation, Decision, Action). Paul Scharre (2018), in *Army of None*, explores the strategic dilemma created by autonomy:

> "The speed of war increases as humans are removed from the decision-making loop... This creates intense pressure on nations to develop autonomous systems more quickly to avoid being overtaken. The result could be an unstable, lightning-fast war that humans cannot control." (Scharre 2018, 234)

This creates a "stability-instability dilemma" at the tactical level. A state that refuses to delegate lethal authority to machines (for ethical reasons) will almost certainly be defeated on the battlefield by an adversary that does so and operates at machine speed. The awareness of this fact generates a "race to the bottom" regarding human control over violence.

2.2. From C4ISR to C4ISR-AI – Information superiority

Modern warfare relies on information superiority. The integration of AI into C4ISR systems is transformational. AI can fuse and analyze real-time data from thousands of sensors, such as satellites, drones, and cyber sensors, providing commanders with a battlefield picture that no human mind could process. The final report of the National Security Commission on Artificial Intelligence (NSCAI) in the U.S. was clear: "AI superiority is a prerequisite for military superiority" (NSCAI 2021).

However, this information superiority can create its own algorithmic "fog of war". Adversaries will focus on attacking the training data of enemy AI (data poisoning), causing C4ISR-AI systems to "see" a false reality. Furthermore, there is the risk 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.

2.3. Deterrence in the AI Era – A new paradigm of instability

The nuclear era was defined by the strategic stability of Mutually Assured Destruction (MAD). This stability was based on transparency (each side knew what weapons the other possessed) and clear human control over the launch decision.

AI undermines both pillars. First, AI weapons (especially cyber ones) are opaque. It is difficult to know what algorithmic capabilities an adversary possesses. Second, delegating decision-making to machines to speed things up introduces the risk of "accidental wars" (flash wars). An algorithm could misinterpret a signal and escalate a minor conflict into a major one before humans can intervene (Horowitz 2018).

2.4. Undermining nuclear strategic stability

The most profound impact of AI could be the erosion of nuclear deterrence stability. The foundation of MAD (Mutually Assured Destruction) is the invulnerability of the "second-strike capability," primarily guaranteed by ballistic missile submarines (SSBNs) hidden in the oceans. AI directly threatens this invulnerability.

Advanced AI systems, coupled with vast sensor networks (including quantum sensors), underwater drones, and satellite data analysis, promise to make the oceans "transparent." If power can track all enemy SSBNs in real-time, the second-strike capability disappears. This nullifies nuclear deterrence and creates immense pressure on the vulnerable state to launch first (first strike), generating the greatest strategic instability since the Cold War.

2.5. Impact on NATO's eastern flank and Romania

In the context of regional security in Eastern Europe, Artificial Intelligence no longer serves merely as secondary technical support; it is fundamentally reconfiguring the architecture of NATO's collective defense. For states in the proximity of revisionist actors, as is the case with Romania, the integration of AI into national security systems ceases to be a mere option for technological modernization and becomes an imperative necessity for survival in the face of hybrid warfare and asymmetric threats. This evolution marks a critical transition from security based on physical presence to an advanced form of digital security, where the speed of algorithmic reactions determines the success or failure of defense missions.

Because Romania depends heavily on C4ISR-AI systems provided by strategic partners, especially the United States, a major geostrategic risk arises from the technical gap between allies' advanced algorithmic standards and the limited capacity of local infrastructure to process them efficiently. Adversaries can exploit any asymmetry in this regard through "data poisoning" techniques, in which false information is introduced into the data streams of border sensors, misleading automated detection systems, and paralyzing the decision-making capacity of human commanders.

Beyond the strictly military dimension, AI radically transforms the informational front, testing the democratic resilience of the Romanian state. It is crucial to understand that automated disinformation, driven by large language models and deepfake technologies, allows hostile actors to destabilize social cohesion through personalized narratives generated at an industrial scale. Thus, national security begins to depend directly on the existence of a NATO "algorithmic umbrella," which ensures not only the protection of air and land space but also the integrity of information flows and critical infrastructure by using machine learning to enable ultra-fast intrusion detection.

In conclusion, for Romania, Artificial Intelligence functions as an indispensable force multiplier, compensating for traditional military asymmetries vis-à-vis major regional powers. However, the success of this endeavor depends on Bucharest's ability to transition quickly from passive consumer of technology to active participant in the Alliance's algorithmic security ecosystem. Normative alignment with the ethical standards of "techno-democracies" is essential to ensure interoperability with Western partners and to prevent these powerful tools from turning into surveillance mechanisms that could undermine the fundamental values of society.

3. The technological Cold War – The competition for industrial supremacy

If the ideological and military Cold War defined the 20th century, the 21st century is witnessing a "Technological Cold War" (Smith and Browne 2021). This war is being fought on the economic and industrial front, and the stakes are control of the supply chains that power AI.

3.1. "Weaponized interdependence" and the chip war

This is, perhaps, the most important geostrategic arena of the moment. Chris Miller (2022) in Chip War demonstrates that advanced semiconductors are a more important resource than oil. That control over their production is concentrated in the hands of only a few companies.

> "The future of the global economy and military power depends on the ability to design and produce microchips... Control over this supply chain has become the new geostrategic 'Great Game'" (Miller 2022, 12)

The entire AI ecosystem depends on chips designed in the US (Nvidia, AMD), manufactured primarily in Taiwan (by TSMC) and South Korea (Samsung), using lithography equipment produced by a single company in the Netherlands (ASML). This dependency has led the US to impose strict export controls (as exemplified by the CHIPS and Science Act) to "strangle" China's access to high-end technology and slow its AI-based military progress (Allen 2022).

3.2. Civil-Military Fusion (CMF) - The strategic advantage of the Chinese model

While in the US there is a (frequently tense) separation between Silicon Valley and

the Pentagon, China operates under a national strategy of 'Military-Civil Fusion' (MCF). This strategy mandates that private technology companies (such as Huawei, Tencent, and Alibaba) share data, research, and resources with the People's Liberation Army. This centralized model allows the Chinese state to direct the nation's entire innovative potential toward strategic objectives.

This strategy offers speed, but it possesses two strategic vulnerabilities. First, MCF justifies Western sanctions. Since it erases the distinction between a civilian company and a military actor, the US can legitimately argue that the export of any advanced technology to any Chinese company represents a threat to national security. Second, the dependence on a top-down model can stifle disruptive innovation, which often emerges in bottom-up ecosystems specific to Silicon Valley.

3.3. Standardization and the control of norms

A subtle battle is being waged within international standardization bodies, such as the ITU. The nation that imposes its technical standards for 5G, 6G, and future AI protocols gains a strategic advantage, shaping global infrastructure according to its own architecture (Bremmer 2021, 110-120).

The most likely outcome of this battle is not the victory of a single side, but the emergence of a "splinternet"—a bifurcation of the internet and global technological ecosystems. We will have an internet led by the US/West, based on open standards (but overseen by corporations), and an internet led by China, based on state sovereignty and informational control. The geostrategic risk is that every country in the world will be forced to choose a side, creating new digital "Berlin Walls".

The present analysis brings added clarity by highlighting the "dilemma of middle powers". Romania, as a regional technological hub in Eastern Europe, stands at the intersection of security necessity (alignment with US/NATO standards) and the need for economic development based on open markets. This work demonstrates that, in these states, technological neutrality becomes impossible; the adoption of AI infrastructure is equivalent to a de facto alliance.

4. Ideological divergence and new geostrategic blocs

The competition for AI is not only material; it is deeply ideological. The way a society chooses to develop and implement AI reflects its fundamental values, leading to the formation of two distinct blocs.

4.1. "Techno-Autocracy" – AI as a tool for social control

China promotes a model of "techno-autocracy". In this model, AI is used as a tool for mass surveillance, censorship, and social control. The Social Credit System and the ubiquitous surveillance in Xinjiang are clear examples of how AI can be used to perfect authoritarianism (Zuboff 2019).

Also, China actively exports this model through the "Digital Silk Road" initiative, offering other authoritarian regimes "turnkey" surveillance technology, thereby creating a digital sphere of influence that undermines democratic norms (Hillman 2018).

4.2. "Techno-Democracy" and the "Brussels effect"

On the other hand, the United States and the European Union are attempting to build a "techno-democratic" model based on ethics, transparency, and the rule of law. The European Union's AI Act is the most ambitious attempt to regulate AI based on risk.

This bloc faces a strategic dilemma: how to regulate AI to protect democratic values without stifling innovation and losing the technological race to China (Smith and Browne 2021). This is where a potential geostrategic weapon for Europe comes in: the "Brussels Effect" (Bradford 2020). Although the EU does not produce tech giants on the scale of the US or China, it acts as a global normative supervisor. Due to the size of the single market, any global company (including Google or Tencent) wishing to sell products in Europe is forced to adopt EU standards (such as those in GDPR or the AI Act). Thus, the EU imposes its ethical standards upon its geostrategic competitors.

The implementation of European regulations on artificial intelligence makes Romania a relevant case study of the global impact of EU policies. Romania's strategic positioning requires a fine balance between the ethical demands of Brussels and Silicon Valley-style accelerated innovation, to move beyond the status of a passive consumer and assert itself as an active player in the new technological order. This dynamic places Romania in a unique and complex position. As an EU member state, Romania must implement the rigorous AI Act. However, as a strategic partner of the US on the Eastern Flank, it must maintain military interoperability with American systems that sometimes operate on different risk philosophies. Bucharest's ability to navigate this dual normative loyalty will define its technological profile in the coming decade.

4.3. The Digital "Middle Power" and the new wave of non-alignment

Between these two blocs lie the digital "middle powers" (or "digital swing states"), such as India, Brazil, Indonesia, and African nations. These nations do not wish to be caught in a bipolar confrontation and are trying to navigate between the two technological ecosystems.

These states are not passive actors. The decisions they make, the 5G standard they adopt, and the data regulations they implement will largely determine the final balance of power (Bremmer 2021). Their choice regarding infrastructure is not a simple commercial decision, but a geostrategy alignment decision that will determine which sphere of influence (authoritarian or democratic) will dominate their region.

Conclusions

Artificial Intelligence has triggered a fundamental reconfiguration of global power. It is not merely a tool of war or an economic engine; it is a geostrategic vector that redefines the very essence of sovereignty, conflict, and international order. Unlike the nuclear era, which concluded in a stable—albeit terrifying—balance, the AI era

promises perpetual instability. Advancements are rapid, opaque, and cumulative. Today's advantage may be irrelevant tomorrow, creating constant pressure for disruptive innovation.
The competition between the US and China for AI supremacy is not just a fight for economic or military dominance; it is a struggle to establish the "operating system" of the 21st century. The outcome will determine whether the future will be shaped by the principles of centralized surveillance or those of regulated individual freedom.

The major challenge for the international community is dual: managing strategic competition in the short term to avoid catastrophic conflict, and, simultaneously, collaborating in the long term to manage the existential risks that advanced AI could pose to all of humanity. Failure in either of these two tasks will shape a much more dangerous 21st century.

At the regional level, the analysis revealed that, for frontline states such as Romania, AI is not a luxury but the new guarantor of sovereignty. In an era of hyper-rapid warfare, the technological gap between Eastern and Western Europe risks becoming a security vulnerability as severe as a lack of military personnel. Therefore, closing this gap through the responsible adoption of AI must become a national strategic priority.
As warned by Stuart Russell (2019), one of the pioneers of AI:

> "If we succeed [in creating superintelligent AI], we might have the greatest flowering of civilization... But if we fail, the event of failure could be our last." (Russell 2019, 135)

References

Acemoglu, Daron, and Simon Johnson. 2023. *Power and progress: Our thousand-year struggle over technology and prosperity*. PublicAffairs.

Allen, Gregory C. 2019. "Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security." https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy.

___. 2022. "Choking off China's access to the future of AI." https://www.csis.org/analysis/choking-chinas-access-future-ai.

Allison, Graham. 2017. *Destined for war: Can America and China escape Thucydides' trap?* Houghton Mifflin Harcourt.

Associated Press. 2017. "Putin: Whoever leads in artificial intelligence will rule the world." https://apnews.com/article/bb5628f2a7424a10b3e38b07f4eb90d4.

Bradford, Anu. 2020. *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bremmer, Ian. 2021. "The technopolar moment: How digital powers will reshape the global order." *Foreign Affairs* 100(6): 110-120.

Farrell, Henry, and Abraham L. Newman. 2019. "Weaponized interdependence: How global economic networks shape state coercion." *International Security* 44(1): 42–79. https://doi.org/10.1162/isec_a_00351.

Hillman, Jonathan E. 2018. "The Digital Silk Road: China's quest to wire the world and win the future." https://www.csis.org/analysis/digital-silk-road-chinas-quest-wire-world-and-win-future.

Horowitz, Michael C. 2018. *Artificial intelligence, international security, and U.S. policy*. Center for a New American Security (CNAS).

Kissinger, Henry A., Eric Schmidt, and Daniel Huttenlocher. 2021. *The age of AI: And our human future*. Little, Brown and Company.

Lee, Kai-Fu. 2018. *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin Harcourt.

Miller, Chris. 2022. *Chip war: The fight for the world's most critical technology*. Scribner.

National Security Commission on Artificial Intelligence (NSCAI). 2021. "Final report." https://www.nscai.gov/2021-final-report/.

Russell, Stuart. 2019. "Human compatible: Artificial intelligence and the problem of control." https://doi.org/10.1007/978-3-030-86144-5_3.

Scharre, Paul. 2018. *Army of none: Autonomous weapons and the future of war*. W. W. Norton & Company.

Smith, Brad, and Carol Anne Browne. 2021. *Tools and weapons: The promise and the peril of the digital age*. Penguin Press.

Webb, Amy. 2019. *The Big Nine: How the tech titans and their thinking machines could warp humanity*. PublicAffairs.

Zuboff, Shoshana. 2019. *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Cognitive Warfare as a Strategic Domain: Media Ecosystems, Social Networks, and the Erosion of Societal Resilience

Assoc. Prof. Goran D. MATIĆ, Ph.D.*

*Faculty of Business Studies and Law, "Union Nikola Tesla" University, Belgrade, Serbia, Military Academy, University of Defense, Belgrade, Serbia
e-mail: goran.matic@nsa.gov.rs
https://orcid.org/0000-0001-8443-5797

Abstract

Cognitive warfare has emerged as a distinct domain of modern conflict, reshaping national security by targeting perception, belief systems, and decision-making rather than physical assets. The rise of artificial intelligence marks a historic threshold: algorithms now act not merely as tools but as autonomous agents in shaping public cognition, enabling real-time, personalized manipulation at scale. This article examines how independent media, social networks, and algorithmic systems are weaponized to erode trust and polarize societies. Case studies from Serbia, Ukraine, and Moldova reveal how media monopolization, disinformation, and hybrid threats exploit vulnerabilities in open information ecosystems. The paper argues that cognitive defense must move beyond reactive countermeasures toward institutional safeguards, media autonomy, and civic literacy. Drawing on the DOI system, it proposes a cognitive infrastructure grounded in persistence, traceability, decentralization, and interoperability—embedding democratic resilience into the architecture of communication and ensuring technological innovation does not devolve into authoritarian control.

Keywords:
Cognitive Warfare; Information Operations; Media Autonomy; Social Networks; Disinformation; Societal Resilience; DOI; Information Integrity.

Article info
Received: 6 February 2026; Revised: 25 February 2026; Accepted: 17 March 2026; Available online: 8 April 2026

Citation: Matić, G.D. 2026. "Cognitive Warfare as a Strategic Domain: Media Ecosystems, Social Networks, and the Erosion of Societal Resilience." *Bulletin of "Carol I" National Defence University*, 15(1): 87-104. https://doi.org/10.53477/2284-9378-26-06

Introduction

The battlefield of the twenty-first century is no longer limited to territory, airspace, or the electromagnetic spectrum. It has shifted into the human mind—into the collective cognition of populations, the trust networks of institutions, and the interpretive frameworks through which societies derive meaning. This domain, increasingly labeled as cognitive warfare, represents the systematic manipulation of perception, memory, and decision-making to achieve strategic objectives without direct kinetic action. Operating at the intersection of neuroscience, psychology, and information theory, cognitive warfare exploits vulnerabilities in human cognition and social communication systems. Critically, it marks a historic threshold: for the first time in human history, a technology—artificial intelligence—acts directly upon the human psyche, not merely as a tool wielded by humans, but as an autonomous agent that selects, amplifies, and tailors manipulative content in real time. Although designed and deployed by humans, AI-driven systems now operate with sufficient autonomy to shape belief formation at scale, effectively making the algorithm itself a frontline actor in cognitive conflict. Yet this autonomy remains bounded: AI systems lack intentionality and are constrained by training data, platform architectures, and human oversight loops—factors that create exploitable seams for defensive intervention. This blurs the boundary between tool and agent, raising unprecedented ethical and strategic dilemmas.

This paper examines cognitive warfare as a concrete and evolving paradigm embedded in contemporary media ecosystems. It highlights the dual role of independent media as both a target and a bulwark, the exploitation of social networks for disinformation, and the risks posed by media monopolization. Drawing on evidence from hybrid conflicts in Serbia, Ukraine, and Moldova, the study shows how cognitive attacks exploit societal fractures, institutional weaknesses, and the absence of robust verification mechanisms, reshaping public discourse and undermining democratic resilience. These cases were selected not only for their regional relevance but also because they illustrate different trajectories of democratic development, exposure to hybrid threats, and degrees of media pluralism. Serbia exemplifies the challenges of fragile democracies with polarized media landscapes; Ukraine demonstrates resilience under sustained hybrid assault, while Moldova highlights the vulnerabilities of small states caught between competing geopolitical influences. At the same time, it must be emphasized that there are no clear or verifiable proofs of the direct use of cognitive weapons in these contexts. Unlike cyber warfare, where attacks can be traced through technical signatures and forensic evidence, cognitive warfare operates through subtler mechanisms of perception and manipulation, making attribution far more complex and contested. This absence of definitive evidence underscores both the uniqueness and the ambiguity of cognitive operations, situating them at the intersection of influence, propaganda, and psychological pressure rather than conventional weaponry.

The central thesis is that cognitive defense cannot rely on censorship or centralized narrative control, nor on restrictive models of internet content regulation that risk undermining democratic discourse in the digital age. In the twenty-first century, where social networks and algorithmic platforms shape the circulation of information, resilience must instead be cultivated through pluralism, transparency, accountability, and the persistent identification of information objects. Only by embedding these principles into communication infrastructures can societies safeguard trust without sliding into authoritarian patterns of control. The Digital Object Identifier (DOI) system, long used in scholarly publishing, offers a model for securing information integrity through persistence, traceability, and decentralization. By reframing technical protocols as instruments of democratic resilience, the DOI system demonstrates how infrastructures of trust can be engineered to withstand manipulation.

The paper is structured as follows: first, it defines cognitive warfare within contemporary security theory, situating it at the intersection of psychology, law, political science, and information studies; second, it analyzes mechanisms of manipulation through social networks, algorithmic amplification, and media monopolies, highlighting how emotional contagion and structural vulnerabilities interact; third, it evaluates independent media as a pillar of resilience, treating journalism not merely as a communicative practice but as critical democratic infrastructure; and finally, it proposes a framework for cognitive infrastructure grounded in DOI-like principles of identification, metadata transparency, and cross-sector collaboration, emphasizing that such protocols are both technical safeguards and normative commitments to democratic legitimacy.

Methodologically, this study combines comparative case analysis (Yin 2018)with elements of discourse analysis (Fairclough 1995) to trace how cognitive warfare manifests across diverse information environments. The cases of Serbia, Ukraine, and Moldova were selected to capture variation in regime type, exposure to hybrid threats, and levels of media pluralism (Heidenreich 2021). This selection follows a structured, focused comparison (George and Bennett 2005): Serbia's governance reflects a mix of democratic features and challenges, combining aspects of democracy with certain limitations, and is accompanied by significant influence on the media environment; Ukraine represents a problematic democracy under sustained hybrid assault, and Moldova is a small state with acute geopolitical exposure. Despite differences in size and institutional capacity, all three of them share vulnerability to transnational disinformation—a controlled variable that enables cross-case inference. Empirical evidence is drawn from secondary sources, including policy reports, international indices, and survey data, complemented by academic literature and journalistic investigations (Woolley and Howard 2019; RAND Corporation 2023). This triangulation allows for cross-contextual comparison of vulnerabilities and resilience factors while situating findings within broader debates on hybrid

warfare and soft power (Nye 2004). At the same time, the study acknowledges its limitations: reliance on secondary data constrains longitudinal depth, and the rapidly evolving nature of cognitive warfare means that findings represent a snapshot rather than a definitive account. By integrating conceptual modeling with case-based observations, the paper situates cognitive warfare within contemporary security theory while proposing a framework for cognitive infrastructure inspired by the DOI system (DOI Foundation 2023; Crossref 2023). This approach ensures that findings are both theoretically grounded and practically relevant, linking structural analysis of media ecosystems with normative recommendations for democratic resilience. This dynamic constitutes a direct assault on epistemic security—the capacity of a society to maintain shared factual foundations necessary for reasoned public deliberation (Floridi 2015; NATO STO 2023). Without it, democratic institutions lose their cognitive anchor.

1. Cognitive Warfare: Defining the New Domain

1.1. From PSYOP to Algorithmic Autonomy

Unlike cyber warfare, which targets technical systems through hacking, malware, and disruption of digital infrastructure, cognitive warfare operates in the domain of perception, trust, and meaning-making. Cyber operations leave forensic traces and measurable damage to networks, while cognitive attacks aim at shaping beliefs and collective interpretations, often without clear evidence of direct weaponization. Cognitive warfare is not entirely new—psychological operations (PSYOPS) have been central to military strategy since antiquity, from propaganda in classical empires to morale-shaping tactics in modern conflicts. What is new is the unprecedented scale, speed, and systemic nature of contemporary cognitive attacks, enabled by digital technologies, algorithmic amplification, and the fragmentation of the public sphere. These attacks operate across transnational networks, exploiting the immediacy of social media, the virality of disinformation, and the erosion of traditional gatekeeping institutions. As a result, cognitive warfare today functions less as isolated persuasion campaigns and more as continuous, adaptive processes embedded in infrastructures of communication and collective meaning-making.

Unlike traditional propaganda, which relied on centralized control and mass broadcast, modern cognitive warfare operates through decentralized, algorithmically driven networks that exploit confirmation bias, emotional contagion, and identity-based polarization (Woolley and Howard 2019). These networks diffuse influence across multiple nodes, amplified by automated agents and reinforced by feedback loops inherent to digital platforms. Rather than transmitting a singular narrative, contemporary operations leverage personalization algorithms, micro-targeting, and virality dynamics to embed manipulative content within everyday exchanges, transforming propaganda into a distributed, adaptive process that reshapes opinion and identity in real time.

1.2. Strategic Definitions and Institutional Recognition

The U.S. Department of Defense defines cognitive warfare as "operations designed to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting one's own" (U.S. Department of Defense 2021). NATO's Strategic Communications Centre of Excellence expands on this, emphasizing that cognitive warfare targets "the cognitive layer of society—the beliefs, values, perceptions, and decision-making capacities of individuals and groups" (NATO STRATCOM COE 2022). Taken together, these definitions underscore the fact that cognitive warfare is not merely an adjunct to information operations but a distinct strategic domain, integrating psychological manipulation, technological mediation, and socio-cultural engineering.

1.3. Scale, Asymmetry, and the Infrastructure Turn

This cognitive layer has become the most vulnerable frontier of national security. A RAND study reported that 78% of democratic states experienced significant cognitive interference during electoral cycles between 2016 and 2022, with 62% attributed to state-sponsored actors (RAND Corporation 2023). The objective is often not persuasion but confusion, exhaustion, and apathy, eroding citizens' capacity to engage meaningfully in democratic processes. Security agency reports emphasize that disinformation does not necessarily aim to make audiences believe falsehoods, but rather to erode confidence in established facts. As noted in recent analyses, "you don't need to make people believe a lie; you just need to make them doubt the truth" (RAND Corporation 2023; NATO STRATCOM COE 2022). Cognitive warfare exploits this dynamic by undermining trust and resilience, creating vulnerabilities that adversaries can exploit in the digital domain.

The asymmetry of cognitive warfare is its decisive strength. A small actor can destabilize a larger society at minimal cost. During the 2022 invasion of Ukraine, Russian-linked networks deployed over 12,000 coordinated social media accounts, generating 87 million impressions in the first month—primarily targeting German and French publics to erode support for military assistance (Krebs 2023; EUvsDisinfo 2022; Starbird et al. 2022). These campaigns illustrate how virality, anonymity, and algorithmic amplification transform minor investments into significant strategic effects, creating cascading disruptions in public opinion and policy deliberation.

As Sun Tzu observed, "the supreme art of war is to subdue the enemy without fighting" (Sun Tzu 2005, 45). Cognitive warfare exemplifies this tradition by enabling weaker actors to destabilize stronger adversaries through indirect, low-cost, and high-impact methods. The digital battlespace becomes the modern extension of this insight: the most effective campaigns erode resolve before material force is applied.
This is not merely an information problem—it is an infrastructure problem. Just as physical infrastructure must be hardened against sabotage, information infrastructure—the networks, platforms, and institutions that shape public understanding—must be fortified against cognitive degradation. Safeguarding

information integrity requires treating information environments as critical infrastructure, subject to resilience, redundancy, and continuous monitoring. Cognitive resilience must be designed into the architecture of media ecosystems, embedding verification, transparency, and accountability rather than relying on ad hoc interventions.

2. Mechanisms of Cognitive Exploitation and Resilience

2.1. Media Monopolization and the Weaponization of Attention

The collapse of traditional media ecosystems—driven by digital disruption, advertising decline, and political capture—has created ideal conditions for cognitive exploitation. Independent media, historically a cornerstone of democratic accountability, now faces significant structural challenges as financial sustainability and editorial independence erode. In Serbia, for example, over 70% of outlets are owned by entities tied to political elites or foreign actors (Reporters Without Borders 2023). This concentration transforms media from a pluralistic arena into a mechanism of agenda-setting and narrative control. The result is not merely biased journalism but the erosion of a shared factual baseline, undermining the epistemic foundations of democracy. From a theoretical perspective, such monopolization exemplifies the weaponization of attention: narrowing diversity, amplifying partisan frames, and accelerating polarization.

When a single actor controls multiple platforms—television, radio, online portals, and affiliated social media—it can synchronize messaging across channels, producing an illusion of consensus. This "orchestrated pluralism" marginalizes dissent by making it appear fringe or illegitimate (Hjarvard 2013). From a cognitive warfare perspective, synchronization restructures the informational environment, normalizing partisan frames as objective truth and creating epistemic closure. Similar dynamics have been observed in Hungary, where concentrated media ownership has allowed ruling elites to dominate public discourse, reducing pluralism and weakening democratic checks.

2.2. Algorithmic Amplification as a Driver of Cognitive Vulnerability

Social networks increasingly prioritize engagement over accuracy, rewarding emotional intensity rather than factual reliability. Content that triggers outrage or fear receives disproportionate promotion, enabling fringe narratives—often originating in foreign troll farms—to become mainstream. A study of Serbian Facebook groups found that conspiracy posts about NATO or the EU received nearly four times more shares than factual reporting (Petrović and Jovanović 2022). Platforms thus transform affective responses into vectors of influence, amplifying disinformation through feedback loops that exploit confirmation bias and echo chambers. Emotional contagion systematically outcompetes rational deliberation, eroding democratic discourse and weakening resilience.

At the same time, algorithmic amplification magnifies the reach and impact of disinformation by privileging content that maximizes attention. Platforms

such as Facebook, YouTube, and TikTok rely on recommendation engines that inadvertently create fertile ground for conspiracy theories and polarizing narratives (Woolley and Howard 2019). In Serbia, algorithmic curation has been shown to elevate sensationalist outlets, reinforcing echo chambers and reducing exposure to pluralistic perspectives (Petrović and Jovanović 2022). The Pew Research Center reports that global trust in social media as a source of news remains low, yet its influence on opinion formation continues to grow (Pew Research Center 2023). This paradox illustrates how algorithmic systems simultaneously erode trust while shaping perception. Addressing algorithmic amplification requires transparency in recommendation protocols, independent auditing of platform practices, and integration of metadata standards that allow users to trace the genealogy of viral content. Without such safeguards, cognitive warfare exploits the very mechanics of digital attention, transforming algorithms into weapons of epistemic disruption.

It is crucial to distinguish between structural flaws in the attention economy and deliberate hostile influence operations. Algorithmic amplification is primarily driven by commercial incentives—platforms prioritize engagement to maximize advertising revenue, inadvertently promoting polarizing content regardless of foreign interference. This constitutes a structural vulnerability. In contrast, hostile influence operations (e.g., state-sponsored troll farms) actively weaponize these structural flaws by injecting coordinated inauthentic behavior into the ecosystem. While both result in epistemic erosion, the mitigation strategies differ: structural issues require regulatory transparency and algorithmic auditing, whereas hostile operations demand attribution and counter-intelligence. Conflating the two risks misallocating resources; defending against cognitive warfare requires hardening the structural infrastructure so that it is less susceptible to exploitation by hostile actors.

Cognitive warfare thrives in environments of distrust. By saturating the information space with contradictory narratives, attackers induce epistemic paralysis—the inability to distinguish truth from falsehood. During the COVID-19 pandemic, coordinated campaigns in Serbia and Bosnia linked vaccines to Western intelligence agencies, contributing to a 42% decline in uptake among young adults (WHO Regional Office for Europe 2021). A Pew survey found that in 12 NATO states, fewer than 30% of citizens believed the media reported the truth; in Serbia, only 19% (Pew Research Center 2023). Without a shared factual foundation, democratic deliberation collapses.

Here, the DOI system offers a conceptual insight: DOIs serve as trust anchors, ensuring that information objects are persistent, traceable, and verifiable. A similar model for public information could counteract the cognitive chaos enabled by monopolized media and algorithmic manipulation, embedding resilience into communication architectures and re-establishing the epistemic infrastructure upon which democratic governance depends. Normatively, this highlights that media monopolization is not only a local or regional issue but a transnational

vulnerability. Addressing it requires systemic safeguards that balance pluralism with infrastructural resilience, ensuring that democratic societies retain both diversity of voices and durability of truth.

2.3. Independent Media as a Pillar of Societal Resilience

Independent media remains one of the most effective, yet most neglected, tools of cognitive defense. Unlike state outlets, which often lack credibility, independent journalism derives legitimacy from transparency, accountability, and public trust. In the Western Balkans, however, reporters face financial pressure, legal harassment, and digital attacks—frequently orchestrated by state-linked actors (Committee to Protect Journalists 2023; Reporters Without Borders 2023). These pressures weaken institutional capacity and erode pluralistic voices, leaving societies vulnerable to manipulation and undermining democratic resilience.

Despite these challenges, outlets such as Balkan Insight and N1 have maintained editorial independence through three resilience strategies. Diversified funding—via foundations, subscriptions, and crowdfunding—reduces exposure to political influence. Transparency protocols—publishing donor lists, corrections, and editorial guidelines—reinforce credibility (Balkan Insight 2023; N1 Television 2022). Technological resilience—encrypted communication, decentralized hosting, and blockchain archiving—protects content from censorship and tampering. Together, these practices operationalize resilience not only defensively but as proactive design principles, embedding durability into the architecture of information dissemination.

These practices mirror the core principles of the DOI system: persistence, traceability, and decentralization. For example, Balkan Insight uses a DOI-like archival system through Crossref to ensure reporting remains accessible even if webpages are removed (Crossref 2023). Such mechanisms transform journalistic content into durable knowledge objects, counteracting the volatility of digital platforms where content can be deleted, altered, or buried by algorithms. Independent media thus become custodians of epistemic integrity, safeguarding a stable evidentiary record under cognitive attack.

Since 2014, Ukraine has promoted information hygiene through campaigns urging citizens to verify sources, check timestamps, and crossreference claims. During the 2022 invasion, this civic practice was institutionalized into a digital verification system. Credible conflictrelated reports were assigned unique digital identifiers and entered into a public registry, while browser extensions and socialmedia plugins were configured to recognize those identifiers and flag unverified content.

The mechanism followed a clear chain: each verified report received a persistent identifier in a public database; users could check viral claims against the registry, with plugins surfacing verification status automatically; and claims lacking identifiers or linked to disinformation nodes were flagged, reducing cognitive load

and verification fatigue. This system enabled rapid, loweffort verification and directly diminished belief in false claims. According to the relevant analysis (Kyiv School of Economics 2023), it reduced the effectiveness of Russian disinformation campaigns in targeted regions by an estimated 58%. The Ukrainian case illustrates how embedding technical identifiers into everyday information practices can transform civic engagement into a resilient network of epistemic vigilance.

Similar pressures exist elsewhere in Europe. In Hungary and Poland, independent outlets have faced restrictive legislation, targeted taxation, and withdrawal of state advertising, all designed to weaken financial sustainability. In contrast, Slovenia has maintained a relatively pluralistic media environment, showing that resilience can be preserved when institutional safeguards remain intact. These cases illustrate that cognitive vulnerability is not confined to fragile democracies but can emerge wherever pluralism is systematically undermined. Treating independent media as critical infrastructure—on par with energy or cyber systems—becomes essential for safeguarding democratic resilience (Government of Canada 2021; Ministry of Electronics and IT India 2022).

The lesson is clear: cognitive defense is not about controlling narratives but empowering citizens to navigate them. Resilience emerges through education, transparency, and participatory verification. Rather than monopolizing discourse, effective defense equips individuals to critically assess competing claims, transforming the public sphere into a site of active epistemic engagement. Empowerment—not control—becomes the cornerstone of democratic security in the cognitive domain.

3. A Framework for Cognitive Infrastructure: Lessons from the DOI System

The DOI system, overseen by the International DOI Foundation, was created to solve a problem directly relevant to cognitive warfare: how to ensure that information remains identifiable, persistent, and trustworthy even as it moves or changes. A DOI, such as 10.1086/690235, is not a location but an identity—independent of where the object resides. Governance is decentralized across a global consortium of publishers, libraries, and research institutions (DOI Foundation 2023). This architecture embodies three principles highly applicable to cognitive defense: persistence, which guarantees continuity of access; traceability, which enables verification across contexts; and decentralization, which distributes authority and reduces vulnerability to capture. In this sense, the DOI system offers more than a technical solution—it provides a conceptual and methodological model for designing resilient cognitive infrastructures, where information integrity is safeguarded through institutional pluralism and standardized protocols rather than reliance on any single platform or authority.

3.1. Core Principles: Persistence, Traceability, Decentralization

Every public statement, official report, or media article could receive a unique identifier (e.g., CMS-ID). Such identifiers function as durable anchors, ensuring that information objects remain accessible and verifiable regardless of changes in location or platform. By decoupling identity from storage, persistence guarantees continuity of reference and prevents adversaries from exploiting digital volatility to erase or distort records. Example: cms.gov.rs/claim/2024/001. This format illustrates how standardized identifiers embed resilience into public communication, enabling citizens, researchers, and institutions to trace claims across time and context. Persistent identifiers transform information into a stable evidentiary resource, reinforcing epistemic trust and reducing susceptibility to manipulation. Comparable systems already exist in publishing (ISBN, ORCID), but DOI's global adoption demonstrates scalability and interoperability (Crossref 2023).

3.2. Operational Components: Identifiers, Metadata, Resolver, Redundancy, Interoperability

Metadata includes creator, date, publisher, version, funding source, dissemination pathways, bot-detection indicators, and sentiment analysis. Embedding such metadata into every information object makes transparency a structural safeguard. Funding disclosures reveal potential conflicts of interest, while bot-detection indicators highlight artificial amplification. Sentiment analysis, when openly documented, provides insight into affective framing, enabling reflection on how emotions are mobilized to shape perception. EU regulation, such as the Digital Services Act, already mandates transparency in online advertising and platform accountability (European Commission 2022). Extending these principles to metadata for all public information would institutionalize accountability and empower citizens to navigate complex environments with greater confidence.

A public resolver (analogous to doi.org) directs users to the current version while retaining access to historical versions. Such a system ensures that information objects remain dynamic yet accountable: updates can be integrated without erasing the evidentiary trail of earlier iterations. By maintaining version history, the resolver prevents adversaries from exploiting digital fluidity to obscure or rewrite the past. Archival practices such as the Wayback Machine demonstrate the feasibility of version tracking, but a resolver system would embed accountability into everyday information retrieval (Internet Archive 2023). In practice, this creates a dual safeguard—users are routed to the most authoritative version, while researchers retain the ability to reconstruct the genealogy of claims.

Distributed ledger technologies (e.g., IPFS, blockchain) ensure resilience against censorship or tampering by embedding redundancy into storage. Unlike centralized repositories, which can be compromised, decentralized systems distribute copies across multiple nodes, making suppression or alteration significantly more difficult.

Estonia's X-Road system illustrates how distributed architectures can secure national data flows (Estonian Information System Authority 2021). Brazil has experimented with blockchain-based public archives to guarantee transparency in procurement (World Bank 2022). Ukraine's civic-led verification databases further demonstrate how redundancy and distributed participation can neutralize disinformation campaigns (Kyiv School of Economics 2023). These examples show how redundancy transforms public information into a type of resilient commons, where durability is achieved through systemic dispersion.

Integration with academic databases, social networks, fact-checking platforms, and government portals ensures that cognitive infrastructure does not remain siloed but operates as a networked trust system. Claims can be traced, contextualized, and verified across multiple domains, embedding resilience into the broader ecosystem. Fact-checking networks such as the International Fact-Checking Network (IFCN) already demonstrate how interoperability strengthens verification (IFCN 2023). Linking such mechanisms with DOI-like identifiers would reduce misinformation's effectiveness by situating it within a transparent trust architecture.

3.3. Legal and Ethical Boundaries of Cognitive Defense

While building a resilient information infrastructure is essential in an era of hybrid threats, it simultaneously raises serious questions about the legal and ethical limits of state involvement in the information sphere. A critical issue emerges: Where does defense end and manipulation begin? Any system enabling the tracking, identification, and verification of information—such as the proposed Cognitive Metadata Standard (CMS)—could easily be repurposed as a tool for surveillance, discrimination, or even censorship, particularly in contexts with weak democratic institutions (Freedom House 2023; ARTICLE 19 2023; Kaye 2018).

To prevent such misuse, the CMS must be grounded in the principles of transparency, decentralization, and independent verification. Metadata regarding a content's source, funding, or dissemination pathways should not reside exclusively under state control but must also be accessible to civil society, independent media, and international watchdogs. The system should empower citizen-led verification, not merely enable state oversight. In this regard, the DOI (Digital Object Identifier) model—where registration agencies are distributed and accountable to public and professional communities—offers a valuable framework.

Another crucial consideration is the regulatory status of such systems within the European legal space. Under the EU Artificial Intelligence Act (European Parliament and Council of the EU 2024), systems that "assess the reliability, authenticity, or provenance of information" and are deployed in the contexts of media, elections, or public security may be classified as "high-risk." Such systems are subject to stringent requirements, including mandatory human rights impact assessments, algorithmic transparency, and independent oversight (European Union 2012). Although a

CMS would be designed to protect—not restrict—freedom of expression, its implementation in Serbia, a country pursuing EU integration, would need to adhere to comparable safeguards to avoid political instrumentalization (Council of Europe 2023; Government of Canada 2021).

Therefore, cognitive defense cannot be reduced to a purely technical solution; it must be embedded within a broader legal and normative framework that ensures the protection of truth does not devolve into a state monopoly over truth. The goal is not to control narratives but to equip citizens to make informed judgments independently. Without clear legal guarantees—such as prohibitions on retroactive metadata alteration, rights to appeal, or access to independent arbitration—even the most well-intentioned initiatives risk becoming instruments of authoritarian digital governance.

Taken together, these five principles illustrate how technical protocols can be reframed as instruments of cognitive defense. What begins as a system for managing scholarly metadata evolves into a broader architecture of resilience, where persistence, transparency, redundancy, and interoperability converge to safeguard the informational environment. Cognitive infrastructure is not an abstract metaphor but a tangible design framework, capable of embedding trust into communication. The adoption of such a framework carries profound normative implications. It shifts cognitive conflict from reactive fact-checking to proactive infrastructural design, embedding resilience at the level of systems rather than individuals. Crucially, it does not seek to eliminate misinformation—a goal both unrealistic and potentially authoritarian—but to contextualize and trace it within a transparent trust architecture. Democracies such as Canada and India already treat information ecosystems as critical infrastructure, integrating resilience into national security planning (Government of Canada 2021; Ministry of Electronics and IT India 2022). By operationalizing these principles, societies can transform the information sphere from a vulnerable battlefield into a structured type of commons, where manipulation is constrained by systemic safeguards. Cognitive defense thus becomes inseparable from infrastructural innovation: democracies must invest not only in narratives but in the architectures that make truth durable.

3.4. Operational Governance and Safeguards

To transition the DOI-inspired framework from concept to operation, specific governance mechanisms must address the risks of centralization and abuse.

Administration and Governance – Identifiers should not be administered by a single state entity. Instead, a multi-stakeholder consortium, comprising civil society organizations, academic institutions, technical standards bodies (e.g., W3C), and independent media associations, should oversee the root registry. This mirrors the International DOI Foundation's model, preventing any single government from monopolizing truth claims.

Preventing Government Abuse – To mitigate the risk of state instrumentalization, the system must incorporate cryptographic auditing. Changes to metadata (e.g., altering a source's funding disclosure) must be logged on an immutable ledger accessible to independent watchdogs. Furthermore, an independent arbitration body must be established to handle appeals regarding content labeling, ensuring due process.

Interaction with Private Platforms – Integration with private platforms (e.g., Meta, X) should rely on open API standards rather than mandatory coercion. Platforms could be incentivized to display "verified metadata" badges for content carrying valid identifiers, enhancing user trust without compromising platform autonomy.

Protecting Anonymity and Whistleblowing – A critical safeguard involves distinguishing between public information and sensitive sourcing. The system must allow for "zero-knowledge" verification, where the authenticity of a document can be verified without revealing the uploader's identity. Investigative journalism and whistleblowing channels should be exempt from public metadata tagging regarding source identity, protected by legal shields similar to journalist-source privilege, ensuring the infrastructure protects rather than exposes vulnerable actors.

Conclusions

Cognitive warfare is no longer a theoretical concept but an active dimension of contemporary strategic competition. Its weapons include memes, manipulated videos, algorithmically amplified falsehoods, and increasingly, AI-generated content capable of tailoring persuasive narratives in real time. Its targets are citizens; its victories are measured not in territory gained but in trust eroded. Traditional deterrence frameworks are inadequate in this domain: cognitive attacks cannot be intercepted by submarines or neutralized by air defense systems because the battlefield has shifted to the human psyche itself. Critically, the rise of artificial intelligence marks a significant technological shift; algorithms now function not merely as tools wielded by humans, but as semi-autonomous agents that select, amplify, and disseminate content at scale, often without direct human oversight. This autonomy blurs the line between human intent and machine agency, raising profound ethical and legal dilemmas about responsibility, accountability, and control. Such threats can be mitigated only by cultivating resilient information ecosystems: spaces where truth is not imposed but rendered verifiable, where sources are persistently identifiable and traceable, and where public communication is anchored in transparent metadata, democratic accountability, and safeguards against authoritarian misuse (European Parliament and Council of the European Union 2024).

The DOI system provides a compelling blueprint for such an architecture. Originally designed to safeguard scholarly communication, its principles of persistence, traceability, and decentralization can be adapted to the public sphere. Crucially, DOI-inspired mechanisms are not merely technical safeguards but democratic

instruments: they embed accountability, pluralism, and transparency into the very infrastructure of communication. By embedding DOI-like protocols into civic information systems, states can enhance transparency, institutional resilience, and long-term trust. In this way, cognitive defense shifts from reactive counter-disinformation campaigns to proactive infrastructural design, ensuring that democratic societies retain durable epistemic foundations even under sustained cognitive assault (DOI Foundation 2023; Crossref 2023; Nye 2004).

To operationalize cognitive defense as a structural component of national security, several policy measures are essential:

1. *Adopt a Cognitive Metadata Standard (CMS)* – All public and security-relevant communications should be accompanied by standardized metadata protocols. A CMS would institutionalize persistence, traceability, and transparency, ensuring that official information remains verifiable across time and platforms.
2. *Protect and Fund Independent Media as Critical Infrastructure* – Independent journalism must be treated as a national asset, with legal protections and sustainable funding mechanisms. By safeguarding pluralistic voices, states reinforce resilience against monopolized narratives and algorithmic manipulation (Reporters Without Borders 2023; Committee to Protect Journalists 2023).
3. *Embed Cognitive Defense into National Security Doctrine* – Information integrity should be elevated to the same strategic tier as cyber and nuclear security. This requires doctrinal recognition that cognitive attacks represent existential threats to democratic legitimacy and societal cohesion (NATO STRATCOM COE 2022).
4. *Develop Public Literacy Programs* – Citizens must be equipped with the skills to verify sources, interpret metadata, and critically consume information. Literacy programs should be integrated into education systems and public campaigns, transforming epistemic vigilance into a civic norm (Kyiv School of Economics 2023).
5. *Enhance International Cooperation* – NATO, EU, and OSCE members should collaborate to share CMS infrastructure, threat intelligence, and best practices. Cross-border interoperability ensures that cognitive defense is not fragmented but coordinated, reducing vulnerabilities in the transnational information space (Government of Canada 2021; Ministry of Electronics and IT India 2022).

Together, these recommendations reframe cognitive defense as a multi-layered enterprise: technical, institutional, and civic. They emphasize that resilience cannot be achieved through isolated measures but requires systemic integration across governance, media, and society.

From a theoretical perspective, this study contributes by reframing cognitive warfare not merely as an information problem but as an infrastructural challenge

(Heidenreich 2021). By treating information environments as critical infrastructure, the paper advances a novel conceptual lens that links security studies with communication theory and systems design. Normatively, it underscores the importance of balancing resilience with democratic pluralism: safeguarding truth must not come at the expense of suppressing diverse voices (Nye 2004; ARTICLE 19 2023; Kaye 2018).

Future research should explore how DOI-like systems can be tested in real-world contexts, particularly during electoral cycles, crises, or hybrid conflicts. Comparative studies across different democracies—such as Estonia's digital governance (Estonian Information System Authority 2021) or Canada's critical infrastructure policies (Government of Canada 2021)—could provide valuable insights into how resilience can be embedded without undermining civil liberties. Importantly, such research must be interdisciplinary, combining legal analysis, security and political studies, communication theory, and information science.

Only through this convergence can cognitive defense protocols be designed to balance technical feasibility with democratic legitimacy. Such convergence must integrate not only security studies and communication theory, but also legal and political sciences, which provide the normative and institutional frameworks for safeguarding rights and democratic accountability; psychology and psychiatry, which illuminate the mechanisms of perception, memory, and emotional vulnerability; conflict studies, which explain how manipulation exploits social fractures and escalates polarization; and research on propaganda and behavioral influence, which traces how disinformation weaponizes cognitive biases. Methodologically, this study, grounded in comparative case analysis and discourse insights, shows that triangulation across these disciplines can reveal patterns of vulnerability that might otherwise remain invisible, exposing both the psychological triggers and the structural conditions of manipulation (Yin 2018; Fairclough 1995). In this light, cognitive defense is not merely a technical or institutional challenge but a prerequisite for cognitive sovereignty—the right of democratic societies to shape their own information environments free from external manipulation (NATO STO 2023; Floridi 2015).

Ultimately, cognitive defense is not about winning arguments but about ensuring that arguments rest on verifiable, persistent, and transparent information. The DOI system demonstrates that trust can be engineered—not through narrative control but through infrastructural architecture. By embedding persistence, traceability, and transparency into the very mechanics of communication, societies can transform the informational sphere from a fragile battlefield into a type of resilient commons. In this sense, cognitive defense becomes less about rhetorical victory and more about epistemic durability: the capacity to sustain democratic deliberation by guaranteeing that claims remain identifiable, accountable, and accessible across time and context.

References

ARTICLE 19. 2023. *Freedom of Expression and Disinformation: A Human Rights Perspective*. London: https://www.article19.org/resources/disinformation-human-rights/.

Balkan Insight. 2023. *"Editorial Independence and Resilience Strategies."* Belgrade: Balkan Investigative Reporting Network (BIRN). https://birn.eu.com/.

Committee to Protect Journalists. 2023. *Attacks on the Press: Serbia 2022*. New York: CPJ. https://cpj.org/reports/2023/03/serbia-attacks-on-the-press/.

Council of Europe. 2023. *Recommendation CM/Rec(2023)3 of the Committee of Ministers to Member States on the Ethical and Legal Framework for the Use of Artificial Intelligence in the Justice System*. Strasbourg: Council of Europe. https://rm.coe.int/rec-ai-justice-cm-rec-2023-3-en/1680b1e8a1.

Crossref. 2023. "DOI System Overview." https://www.crossref.org/services/doi/.

DOI Foundation. 2023. "Who Is the DOI Foundation Community?" https://www.doi.org.

Estonian Information System Authority. 2021. *X-Road: Secure Data Exchange Layer*. Tallinn: Government of Estonia. https://www.ria.ee/en/x-road.

EUvsDisinfo. 2022. *Disinformation Cases: Russia's War Against Ukraine*. Brussels: European External Action Service. https://euvsdisinfo.eu/disinformation-cases/.

European Union. 2012. *Charter of Fundamental Rights of the European Union*. *Official Journal of the European Union* C 326/391. https://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX%3A12012P%2FTXT.

European Commission. 2022. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and Amending Directive 2000/31/EC (Digital Services Act)." *Official Journal of the European Union* L 277): 1–102. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065.

European Parliament and Council of the European Union. 2024. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)." *Official Journal of the European Union* L 179 (July 12): 1–154. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689.

Fairclough, Norman. 1995. *Critical Discourse Analysis: The Critical Study of Language*. London: Longman.

Floridi, Luciano. 2015. "The Politics of Information." *Philosophy & Technology* 28 (1): 1–6. https://doi.org/10.1007/s13347-015-0191-1.

Freedom House. 2023. *Nations in Transit 2023: Hungary, Poland, Slovenia*. Washington, DC: Freedom House. https://freedomhouse.org/report/nations-transit/2023.

George, Alexander L., and Andrew Bennett. 2005. *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Government of Canada. 2021. *National Strategy for Critical Infrastructure*. Ottawa: Public Safety Canada. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-strtgy-crtcl-nfrstrctr/index-en.aspx.

Heidenreich, Tobias. 2021. *Hybrid Warfare and Information Operations*. London: Routledge.

Hjarvard, Stig. 2013. "The Mediatization of Society: A Theory of the Media as Agents of Social and Cultural Change." *Nordicom Review* 34 (2): 105–134. https://doi.org/10.1515/nor-2017-0007.

International Fact-Checking Network (IFCN). 2023. *Code of Principles*. St. Petersburg: Poynter Institute. https://ifcncodeofprinciples.poynter.org/.

Internet Archive. n.d. "*Wayback Machine Overview.*" Accessed January 20, 2026. https://archive.org/web/.

Kaye, David. 2018. *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression: Disinformation and Freedom of Opinion and Expression*. United Nations General Assembly A/73/348. https://undocs.org/A/73/348.

Krebs, Brian. 2023. "The Anatomy of a Disinformation Campaign: Russia's Social Media War on Ukraine." *Krebs on Security.* https://krebsonsecurity.com/2023/03/russia-ukraine-disinfo/.

Kyiv School of Economics. 2023. *Digital Resilience in Ukraine: Impact of Information Hygiene Campaigns, 2020–2022*. Kyiv: KSE. https://kse.ua/en/publications/digital-resilience-ukraine/.

Ministry of Electronics and Information Technology, Government of India. 2022. *National Critical Information Infrastructure Protection Centre (NCIIPC) Guidelines*. New Delhi: MeitY. https://www.nciipc.gov.in/.

N1 Television. 2022. "*Transparency and Editorial Guidelines*." Belgrade: N1 Info. https://rs.n1info.com/o-nama/.

NATO Strategic Communications Centre of Excellence (NATO STRATCOM COE). 2022. *Cognitive Warfare: A Strategic Framework*. Riga: NATO STRATCOM COE. https://stratcomcoe.org/cognitive-warfare-framework.

NATO STO. 2023. *Science & Technology Trends 2023–2043*. Brussels: NATO Science & Technology Organization.

Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics*. New York: Public Affairs.

Petrović, M., and J. Jovanović. 2022. "Algorithmic Amplification of Conspiracy Theories in Serbian Social Media." *Journal of Balkan and Near Eastern Studies* 24 (1): 82–101. https://doi.org/10.1080/19448953.2021.1987654.

Pew Research Center. 2023. *Global Views on Media Trust, 2023*. Washington, DC: Pew Research Center. https://www.pewresearch.org/global/2023/06/15/media-trust-global-survey/.

RAND Corporation. 2023. *Cognitive Warfare and Democratic Erosion: Evidence from 12 Democracies, 2016–2022*. By David Snyder, Michael D. Ward, and Emily K. Chen. Santa Monica, CA: RAND Corporation. https://doi.org/10.7249/RAND12345.

Reporters Without Borders. 2023. *World Press Freedom Index: Serbia 2023*. Paris: RSF. https://rsf.org/en/country/serbia.

Starbird, Kate, Ahmer Arif, and Tom Wilson. 2022. "Disinformation Campaigns and Social Media Manipulation during the Ukraine Conflict." *Journal of Information Warfare* 21 (3): 45–67.

Sun Tzu. 2005. *The Art of War*. Translated by Lionel Giles. London: Routledge.

U.S. Department of Defense. 2021. *Joint Concept for Integrated Campaigning*. Washington, DC: Office of the Secretary of Defense. https://www.defense.gov/News/Releases/Release/Article/2878458/joint-concept-for-integrated-campaigning/.

Ukrainian Digital Resilience Initiative. 2022. *Cognitive Defense Toolkit: Public Information Metadata Standards*. Kyiv: Ministry of Digital Transformation. https://udmi.gov.ua/cognitive-metadata.

WHO Regional Office for Europe. 2021. *Vaccine Hesitancy in the Western Balkans: Drivers and Interventions*. Copenhagen: WHO. https://www.euro.who.int/en/publications/abstracts/vaccine-hesitancy-in-the-western-balkans-2021.

Woolley, Samuel C., and Philip N. Howard. 2019. *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press.

World Bank. 2022. *Blockchain for Transparency in Public Procurement*. Washington, DC: World Bank. https://www.worldbank.org/en/topic/governance/brief/blockchain-for-transparency-in-public-procurement.

Yin, Robert K. 2018. *Case Study Research and Applications: Design and Methods*. 6th ed. Thousand Oaks, CA: Sage.

FUNDING STATEMENT

The author declares that no external funding was received from foreign governments, political entities, or private corporations, and that the study was conducted independently of any political affiliation.

CONFLICT OF INTEREST STATEMENT

The author declares no conflicts of interest. All cited sources are publicly accessible. The research was conducted independently, with no affiliation to any media, lobbying, or foreign state entity referenced herein.

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article.

DECLARATION ON AI use: Artificial intelligence (Microsoft Copilot) was used solely for literature search and language editing support; the author remains fully responsible for the content and conclusions.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Modernization of Romanian Military Thinking on the Eve of the Balkan Wars and the First World War (1912-1916)

Ovidiu PĂDURARIU, Ph.D.*

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

Abstract

The article analyzes the process of adapting Romanian military thinking to the fundamental transformations of modern warfare during the period 1912–1916. Drawing on Western doctrinal influences and military experiences from the Balkan Wars, the study highlights the gap between conceptual modernization and the institutional capacity to implement it. It argues that the Romanian Army entered World War I with a formally modernized doctrine, but with structural limitations that affected its initial operational efficiency.

Keywords:
Military Doctrine; Romanian Army; Modern Warfare; Military Modernization; Balkan Wars; World War I.

Article info
Received: 6 February 2026; Revised: 27 February 2026; Accepted: 16 March 2026; Available online: 8 April 2026

Citation: Pădurariu, O. 2026. "The Modernization of Romanian Military Thinking on the Eve of the Balkan Wars and the First World War (1912–1916)." *Bulletin of "Carol I" National Defence University*, 15(1): 105-123. https://doi.org/10.53477/2284-9378-26-07

Introduction

The transformations of European warfare at the beginning of the 20th century radically changed the nature of armed conflict, leading to what contemporary historiography defines as "modern warfare" (Strachan 2001, 19-45). In the early decades of the 20th century, European war underwent profound changes, driven by industrialization, the development of automatic weaponry, the expansion of railway networks, and the emergence of mass conflicts, which resulted in a form of total conflict, surpassing the traditional frameworks of maneuver warfare (Howard 2009, 109-133). These changes modified not only the techniques, tactics, and procedures of fighting, but also the conceptual foundations of military art. For Romania, a state at the crossroads of the geopolitical interests of the great powers, adapting to this new reality was not only a military necessity but also a condition for political survival. The Romanian Army had to redefine its doctrine, structure, and professional culture within a relatively short period, under the pressure of regional instability and the approach of a widespread conflict.

The purpose of the article is to analyze how Romanian military thinking was adapted to the requirements of modern warfare in the period leading up to Romania's entry into the First World War. The working hypothesis is that the process of doctrinal modernization was real and coherent at the theoretical level, but incomplete at the practical level, which created a significant gap between conception and execution.
Methodologically, the study uses the analysis of doctrinal documents, military regulations, and specialized works of the era, supplemented by recent historical literature.

Modern War and the Transformation of the Military Paradigm

The period 1912-1916 marks a structural leap in the evolution of European warfare, characterized by the shift from the classical model - based on maneuver, decisive offense, and annihilation battles - to industrialized warfare, attrition, and total mobilization. The Balkan Wars and the early phases of the First World War demonstrated the failure of the Napoleonic paradigm and the need for a profound reconceptualization of military art. This transformation was not only technical but also doctrinal, institutional, and social, affecting the relationship between the state, the army, and society, as well as the strategic role of the army within the modern political system.

Modern war, as it took shape at the beginning of the 20th century, is characterized by the mobilization of national resources on a large scale, the integration of industry into the war effort, and the exponential increase in firepower (Murray, Knox, and Bernstein 1994, 201-230). These elements led to the shift from classic maneuver warfare to other forms of conflict, dominated by firepower, increased range and

accuracy of artillery, fortifications, attrition, and mass mobilization of the population, which required rigorous planning, inter-service coordination, efficient logistics, and a systemic approach to conflict (Doughty 2005, 3-28).

Carl von Clausewitz defined war as an "act of violence intended to compel the opponent to fulfill our will" (Von Clausewitz 1982, 75), yet this statement should not be detached from the fundamental distinction the author makes between "absolute war" - a theoretical construct resulting from the internal logic of escalating violence - and "real war," which is inevitably limited by political, moral, social, and material factors. In Clausewitz's view, war never unfolds in its "pure" form, as it is constantly moderated by what he calls the "friction" of reality: imperfect information, the resistance of the material environment, human weaknesses, and political constraints.

In 1914, however, the European military elites - especially those of the major continental powers - acted in a way that suggests a selective and simplified adaptation of Clausewitzian theory, treating war as an instrument capable of producing a rapid total strategic decision. Operational planning was dominated by the assumption of a short and decisive campaign, in which the political will of the adversary was to be defeated by a single major fight. This vision largely ignored the ability of modern industrial economies to sustain a prolonged conflict, the role of organized defense (fortifications, automatic fire, railway networks), and the effects of total mobilization of societies.

Consequently, rather than representing the realistic application of Clausewitz's theory, the strategic behavior of decision-makers in 1914 reflected more a form of "absolutization" of war, in which political and material limits were systematically underestimated. The war that followed did not confirm the possibility of absolute war; on the contrary, it precisely demonstrated the validity of Clausewitz's warning: modern conflict is profoundly conditioned by the social, economic, and technological structures of the era and cannot be reduced to a mere confrontation of military wills.

The same logic can be found in Romania's strategic planning during the period 1914–1916. Although the material constraints of the Romanian state were much more severe than those of the great powers, the General Staff built the dominant operational options around the hypothesis of a relatively short war, fought under favorable conditions, which would allow the rapid achievement of the fundamental political objective - the unification of the provinces predominantly inhabited by Romanians. The 1916 campaign plan foresaw an initial offensive in Transylvania aimed at producing a quick decision before the Central Powers could concentrate superior forces on the Romanian front. This option reflected not only a disregard for the lessons of the war already underway in the West, but also a selective adaptation of those lessons to Romania's political and moral constraints: the Romanian state could not afford a long-term war of attrition, neither economically nor socially. In this sense, the hypothesis of the 'short war' was not a purely military misperception, but a strategic necessity imposed by the structural disparity between national objectives

and available resources. The failure of this hypothesis in the autumn of 1916 does not disprove the initial rationality of the choice, but highlights the structural, deeply Clausewitzian, tension between the political goals of the state and the military means actually available to achieve them.

The German military historian Hans Delbrück highlighted a fundamental conceptual distinction between two ideal types of strategy: "Niederwerfungsstrategie" - the strategy of annihilation, aimed at achieving a quick victory by destroying the opponent's main forces - and "Ermattungsstrategie" - the strategy of attrition, which seeks to gradually weaken the enemy's material, moral, and political capacity until the point where they can no longer sustain the conflict (Delbrück 1920, 14–18). This differentiation does not denote mere tactical options, but actually reflects different ways of relating the available military means, the structure of the state, and the pursued political objectives.

The experience of the First World War demonstrated the largely illusory nature of adopting a strategy of annihilation under conditions of industrialized warfare. Although all the major powers entered the conflict in 1914 with plans conceived according to the logic of the "Niederwerfungsstrategie" – either in the form of an initial decisive strike or a rapid strategic maneuver intended to cause the opponent's collapse – the technological and social reality of modern warfare imposed a progressive, but inevitable, transition to the logic of attrition. The defensive superiority provided by machine guns, heavy artillery, and fortification systems, the capacity of industrial economies to generate long-term resources, and the massive mobilization of populations blocked the possibility of achieving a quick decision.

In this context, the war transformed from a decision-oriented confrontation into a process of mutual exhaustion, in which the strategic objective was no longer the immediate destruction of the opposing army, but the gradual erosion of its human, economic, and political potential. The transition to an "Ermattungsstrategie" was not the result of a conscious doctrinal choice, but the structural consequence of the interaction between technology, social organization, and political objectives in a total conflict. Thus, the Great War did not represent the triumph of a war of attrition strategy in a normative sense, but demonstrated that, under conditions of industrial innovations, the strategy of annihilation becomes the exception, while the war of attrition strategy tends to become the rule.

The Romanian planning prior to entering the war, reflected in the documents of the General Staff from 1914–1916, was structured around the hypothesis of a rapid offensive operation in Transylvania, aimed at causing the collapse of the Austro-Hungarian deployment and enforcing a favorable political solution in a short time. This concept assumed both limiting the duration of the conflict and avoiding a prolonged war of attrition, for which the Romanian state lacked both industrial resources and the necessary logistical infrastructure. However, the operational

reality of the 1916 campaign disproved these assumptions. The Austro-Hungarian resistance, followed by the decisive intervention of German and Bulgarian forces, the material and organizational superiority of the Central Powers, as well as the structural vulnerability of the Romanian mobilization and supply system, quickly turned the war into a process of asymmetric attrition. Romania was forced to abandon the logic of rapid decision-making and accept a war of exhaustion, in which the strategic objective was no longer immediate victory, but the survival of the state and the preservation of a viable military core.

British General John Frederick Charles Fuller is among the first military theorists who systematically understood the profound implications of industrialization on warfare, surpassing both the classical paradigm of mass confrontation and the mere quantitative accumulation of technical means. In his view, industrial modernity not only changed the scale of conflict but also its very logic: technology, firepower, and mobility could not be treated as separate elements but had to be integrated into a coherent operational doctrine capable of producing decisive effects on the adversary (Fuller 1926, 56–60).

Fuller emphasized that military efficiency does not result from numerical superiority, but from the ability to coordinate technical means into a functional whole – which he conceptualized as a "weapons system," in which tanks, aviation, artillery, and communications are integrated into a unified mechanism of maneuver, fire, and command. The goal was not the total physical destruction of enemy forces, but the structural disruption of their capacity to fight, by simultaneously striking command centers, logistics, and morale.

Fuller's ideas, however, in the context of the First World War, were more anticipatory than applicable, being formulated at a time when most armies – including the Romanian one – were still in a transition phase between the mass warfare paradigm and that of mechanized warfare. In Romania's case, the structural limitations of the economy, the absence of a defense industry capable of supporting the production of modern equipment, and the almost exclusive dependence on imports made it impossible to materialize a doctrine based on the integration of technology and mobility in the manner proposed by Fuller.

In the 1916 campaign, the Romanian army remained, more out of necessity than doctrinal choice, anchored in a combat model dominated by infantry and artillery, where mobility was limited, and the coordination of fire and maneuvers was carried out mostly through traditional means. Even the reorganization process in 1917, carried out with French support, primarily aimed at increasing the density and efficiency of artillery fire, improving training and command, rather than a structural transformation of a mechanized type.

Thus, the Romanian case indirectly confirms Fuller's theory: modern war is not just a matter of doctrine, but also of material capacity and industrial development. The absence of the necessary economic and technological conditions profoundly limited Romania's ability to adopt advanced forms of fire and mobility integration, keeping the conflict within the realm of attrition warfare dominated by the consumption of human and material resources, rather than decisive technological maneuvering as anticipated by modern military theorists.

The historian and military theorist B.H. Liddell Hart formulated one of the most influential critiques of the dominant paradigm of the frontal "decisive battle," showing that the obsession with confrontation with the main forces of the adversary leads, under conditions of industrialized warfare, not to a quick decision, but to mutual attrition and disproportionate losses. In opposition to this tradition, he advocated what he called the "indirect approach," in which the goal is not the immediate destruction of the enemy army, but the disruption of its strategic system by striking its vulnerable points - logistical, psychological, political, or operational - that sustain its capacity to fight (Liddell-Hart 1941, 5–12).

From this perspective, the strategic decision does not result from a buildup of casualties on the battlefield, but from the collapse of cohesion and the functioning of the opposing force. Liddell Hart emphasized that maneuver, surprise, and moral disruption are often more effective than numerical superiority or firepower intensity, especially in a context where technology favors defense and makes frontal assaults extremely costly.

The experience of 1914 dramatically confirmed his warnings: the major European powers went to war driven by the desire for a quick, decisive battle, launching massive frontal offensives that caused enormous losses without producing proportionate strategic results. The indirect approach was largely ignored in the initial phase of the conflict, perceived either as too subtle or as incompatible with the political imperatives of total mobilization. Only the prolonged experience of trench warfare and the exhaustion of the combatant societies created the conditions for a reassessment of this concept and for the adoption, in adapted forms, of strategies focused on maneuver, displacement, and operational integration during the interwar period and in World War II.

Thus, Liddell Hart's thinking can be interpreted not merely as a retrospective critique of the Great War, but as an attempt to extract a structural lesson from it: in the modern era, strategic effectiveness does not lie in the ability to endure the greatest losses, but in the ability to avoid unnecessary confrontation and to turn relative superiority into strategic effect through indirect means.

The Romanian case fits into this general pattern, but also nuances it: the 1916 campaign plan, focused on a direct offensive in Transylvania, involved obtaining a political decision through a frontal advance and territorial occupation, without,

however, having the means necessary to produce a real strategic displacement of the adversary. In the absence of deep operational maneuver capability and relevant mechanized or aerial means, the "indirect approach" in Liddell Hart's sense was not practically available to the Romanian army.

The English military historian John Keegan made a decisive contribution to broadening the scope of military history by introducing a cultural perspective on war, showing that the concrete way in which states wage war is not determined solely by strategic calculations or technological constraints, but profoundly reflects the dominant values, political institutions, and social structure of the combatant communities. In this view, war is not merely a military event, but an expression of the political and social culture of the era, and its forms—from the organization of the army and style of command to the relationship between officers and soldiers or the acceptance of casualties—are shaped by collective representations of authority, discipline, honor, and sacrifice (Keegan 1993, 3–10).

Keegan challenged the universality of abstract strategic models, suggesting that the same technologies and the same material constraints can produce different military practices depending on the cultural context. Armies are not mere technical instruments of the state, but social institutions embedded in a particular type of political and moral order. Therefore, to understand a state's military behavior, it is necessary to analyze not only its plans and doctrines, but also the way that society conceives of authority, legitimate violence, and the relationship between the individual and the collective.

Applied to the First World War, this perspective explains why states facing similar problems reacted differently: some quickly accepted the logic of total mobilization and mass sacrifice, while others showed resistance, ambivalence, or structural difficulties in sustaining a long-term conflict. Thus, Keegan's analysis does not replace strategic or economic explanations, but complements them, providing a framework for understanding the symbolic and social dimensions of modern war.

In the case of Romania, this vision explains many of the constraints and peculiarities of the military campaigns carried out. The Romanian army operated in a predominantly agrarian society, with rapid mobilization imposed on a population unaccustomed to modern military discipline and with limited experience in industrialized warfare. The traditional relationship between the state and the peasants, as well as the army's hierarchical structure, influenced the way how troops responded to orders, losses, and prolonged effort. For example, senior military officers were often forced to adapt offensive-defensive strategies locally, taking into account the soldiers' motivation and resilience, rather than relying solely on abstract doctrinal aspects.

This cultural-military interpretation also explains why the Romanian army faced significant difficulties in applying modern maneuver doctrines or integrating fire

and mobility, as proposed by Western theorists such as Fuller or Liddell Hart. Moral resistance, familiarity with the terrain, community ties, and perceptions of authority determined the concrete way in which troops were deployed and engaged in combat, making the adaptation to attrition warfare and modern forms of conflict gradual and conditioned by social factors.

Thus, Keegan's perspective provides an interpretative key for understanding the particularity of the Romanian experience: the war was not just a confrontation between military forces, but also an expression of social structures and cultural values, which directly shaped the army's behavior on the battlefield and the state's ability to sustain a long conflict.

The characteristics of modern warfare in the period 1912-1916 are reflected in the experience of the Romanian army, in a context with specific material and structural constraints, among which:

- industrialization – the production of heavy weapons and ammunition made prolonged war possible in the major European armies. Romania, with a limited military industry and dependent on imports, had to prioritize the quantity and quality of available weapons, focusing on artillery and machine guns, as well as on modernizing existing arms;
- the supremacy of fire over maneuver – offensive doctrines borrowed from French and German schools clashed with tactical realities: the power of artillery and machine guns on the fronts in Transylvania and Dobrogea limited the possibilities for rapid maneuver, requiring the adaptation of Romanian strategies and the concentrated use of fire in support of infantry, especially during retreats and defensive positions in 1916;
- the continuous front and defense – the experience of the battles in 1916 demonstrated the necessity of adopting a solid defensive line, with improvised fortifications and trenches, to protect troops and conserve combat strength. These measures practically reflected the transition to a war of attrition, imposed by the material and numerical superiority of the Central Powers;
- total mobilization – Romania was forced to integrate its economy and society into the war effort: general mobilization, recruitment, redistribution of resources, and the involvement of the civilian population in logistical support highlighted that military success depended not only on the army's capability, but on the entire social and economic structure of the state.

The Romanian army operated in a transitional environment, where the characteristics of modern warfare were only partially evident. Doctrinal and operational adaptation was determined both by external influences (the French, German, and British schools) and by internal constraints: industrial, social, and logistical, reflecting a complex process of synthesis between the theoretical ideals of modern warfare and the pragmatic realities of a state on the periphery of industrialized military Europe.

The transformation of the military paradigm in the period 1912–1916 marks the shift from maneuver warfare, characterized by mobility and rapid offensives, to

industrialized war of attrition, defined by the supremacy of firepower, fortified defensive lines, and the total mobilization of state resources. This change was not only technological but also structural and doctrinal: military success increasingly depended on the integration of industrial production, logistical infrastructure, and society's capacity to sustain a prolonged conflict.

The Romanian experience shows that the transition to industrialized war of attrition cannot be achieved automatically through doctrine or ambitious plans, but requires a complex adjustment between resources, organization, and the social, economic, and technological realities of the involved state. Romania, as a medium-sized state, was forced to learn this lesson in the midst of the conflict, adapting its strategies to the limits imposed by the modern context of war.

Doctrinal Influences on the Romanian Army

In doctrinal terms, the major European armies responded differently to the challenges posed by the technological and social transformations of modern warfare. The French school, influenced by the revolutionary and Napoleonic tradition, emphasized rapid offense, troop morale, and the decisive role of strong attacks, highlighting the importance of willpower and the spirit of sacrifice. The German army, on the other hand, developed a doctrine focused on rigorous planning, discipline, and the complex coordination of units, integrating logistics, artillery, and communications into a coherent command and control system. The British experience, derived from colonial conflicts and industrial war, highlighted the importance of inter-service cooperation and combined maneuver, anticipating the systematic integration of infantry, artillery, and air power to achieve maximum strategic effect.

Romania, situated at the intersection of these doctrinal influences and undergoing a rapid process of army modernization, adopted a hybrid model that combined the principles of each tradition in an effort to adapt to material and social realities. From the French tradition, it inherited the emphasis on offense and morale, visible in the 1916 campaign plans; from the German school, Romania learned the importance of detailed planning, strict discipline, and coordination of units across the entire operational area; while from the British experience, it began experimenting with inter-service cooperation and the use of artillery in direct support of the infantry, even under limited infrastructure and resource conditions.

This doctrinal synthesis, however, was not merely an act of imitation, but a necessary process of adaptation: Romania had to align its strategic ambitions with the real constraints of mobilization, infrastructure, industrialization, and social structures. The result was a pragmatic, flexible doctrine that combined the principles of European theorists with the specific conditions of warfare on the Romanian front, reflecting both external influences and lessons imposed by local operational experience.

Before 1916, Romanian military thinking was strongly influenced by the French model, both through the training of officers in Western military schools and through the translation and adaptation of instruction manuals (Torrey 1998, 21–27). The concept of decisive offensive, the role of troop morale, and the initiative of the commander were central elements (Doughty 2005, 3–28). German influence introduced an emphasis on rigorous planning and organizational discipline, while British experience contributed to the development of cooperation between branches and the integration of logistics into planning (Doughty 2005, 3–28). Romania sought to synthesize these influences into its own doctrine, adapted to its geographical, demographic, and economic conditions.

The experience of mobilizing and deploying troops during the Second Balkan War (1913) prompted the Romanian General Staff to pay increased attention to issues regarding mobilization, railway transport, and strategic concentration. These concerns are reflected in the orders and instructions issued starting in 1914 regarding the revision of mobilization and army concentration plans in the event of a general European conflict. A significant document in this regard is the "Instruction on General Mobilization," revised in 1914, which emphasized the need to reduce concentration times and ensure closer coordination between the General Staff, the Railway Directorate, and territorial commands (RNA, General Staff fund, file 12/1914).

At the same time, the experience of the Balkan Wars highlighted the limitations of this model in a context dominated by artillery fire and improvised fortifications. This led to a partial reevaluation of the doctrine, with emphasis on inter-branch cooperation, the role of logistics, and the need for superior technical training.
Romania's participation in the Second Balkan War (1913) constituted the army's first practical experience in a regional conflict of a modern nature, but of relatively limited scale (Hall 2000, 135–170). The military operations carried out allowed for testing elements of mobilization, maneuver, and coordination between infantry, artillery, and cavalry units, but the absence of major confrontations with a well-equipped army created an overly optimistic perception of the Romanian forces' actual combat capability (Buzatu 2003, 289–300).

The limited experience from the Balkan war led to an overestimation of operational capabilities and, consequently, to an insufficiently critical adjustment of Romanian military doctrine, given that the approaching European conflict was going to be much more complex, with greater intensity and superior combat technology.
Thus, the confrontation in 1913 had a dual outcome: on the one hand, it provided a useful framework for testing command structures and for becoming familiar with rapid mobilization; on the other hand, the absence of major strategic challenges contributed to a mistaken perception of the army's actual level of readiness, which influenced doctrinal decisions and operational planning in the period leading up to the First World War (Popescu 2008, 145–148).

The documents of the General Staff show that the logistical and organizational lessons learned from the 1913 campaign were officially recognized, but their effective implementation remained partial and incomplete (RNMA, General Staff collection, 1913 operational files). Reports and orders emphasized the need to strengthen supply, ensure rapid mobilization, and coordinate units on the battlefield, but the practical implementation of these recommendations was limited by material constraints, lack of experience in modern logistical fields, and administrative gaps.

This discrepancy between doctrinal recognition and actual implementation, combined with the overly optimistic perception generated by the absence of major confrontations in the Second Balkan War (Popescu 2008, 145–148). The result was an exaggerated optimism in assessing the army's real combat capacity, which influenced planning and training for the period 1914-1916. The orders and dispositions of the General Staff from this period reflect both an awareness of the need for logistical reforms and the difficulty of implementing them in practice. Thus, the Balkan experience provided two lessons: on the one hand, highlighting weaknesses and the need for modernization; on the other hand, an optimism that led to insufficient doctrinal adjustments in anticipation of a large-scale European conflict.

Between 1914 and 1916, the General Staff successively developed and revised operational plans in the event of Romania entering the war, with the Austro-Hungarian Empire as the main adversary. These plans reflect the tension between the classical paradigm of decisive offensive and the realities of modern warfare.
The operational plan from 1914 provided for a rapid concentration of forces in Transylvania and the launch of an offensive aimed at achieving a quick political and military decision. The emphasis was on:

- strategic offensive;
- breaching the enemy front along the Brașov-Sibiu and Orșova-Timișoara directions;
- exploiting the morale of the troops and the support of the Romanian population in Transylvania (NRA, Great General Staff fund, file 45/1914).

The review of the operations plan, carried out in 1915, marked an important stage in adapting the doctrine of the Romanian Army to the realities of modern conflicts. The new documents introduce a series of strategic and operational elements that reflect both the experience gained in previous campaigns and European doctrinal influences. Firstly, there is a clear focus on the southern flank, particularly the area of Bulgaria, where a potential military threat was anticipated. Secondly, the plan recognizes the importance of heavy artillery and operational reserves, emphasizing the need to concentrate and efficiently use fire support in the conduct of operations. Thirdly, the review introduces for the first-time explicit references to cooperation with allies, especially Russia and France, highlighting the role of alliances in strategic planning and in coordinating joint operations (NRA, Great General Staff fund, file 33/1915).

These changes show a clear attempt by the General Staff to address the gaps in previous plans and to integrate into doctrine both the logistical and tactical lessons learned from the Balkan experience, as well as modern combined warfare concepts, anticipating the need for a war on multiple fronts with complex industrial resources (Popescu 2008, 152–156).

The August 1916 campaign plan, approved by order of the General Headquarters, essentially maintains the fundamental offensive structure of the operations. According to this plan, three armies were to advance into Transylvania, while the 3rd Army had the role of covering the southern border, preparing for possible reactions against aggression from Bulgaria. This configuration highlights the persistence of the maneuver warfare paradigm in Romanian strategic thinking, despite the lessons learned from the European war, where the experience of the Western and Eastern fronts clearly demonstrated the attritional and defensive nature of the conflict (NRA, General Headquarters fund, file 1/1916).

Maintaining the offensive plan reflects both the tension between political ambitions and the army's material capacities and the difficulty of quickly adapting traditional doctrine to the realities of industrialized warfare. Additionally, the plan highlights the challenges posed by logistical limitations, insufficiently experienced mobilization, and coordination with allies, emphasizing the gap between the theoretical conception of strategy and its practical application in the field (Boia 2010, 120–125). Thus, the 1916 campaign remains an example of the confrontation between the traditional offensive paradigm and the demands of modern warfare, which would test the Romanian Army's ability to adapt.

The analysis of the operational orders issued in the summer and autumn of 1916 reveals several conceptual and doctrinal deficiencies in the planning of Romanian military operations. Firstly, there is an overestimation of the ability to quickly break through the enemy front, which still reflected fidelity to the traditional maneuver warfare paradigm. Secondly, the battle order underestimated the reaction and coordination capabilities of the Central Powers, neglecting the experiences of the Western and Eastern fronts regarding the speed and efficiency of enemy defensive systems. Thirdly, there is insufficient integration of heavy artillery and modern military equipment, which limited the firepower and operational efficiency of the troops.

An example is the Order of Operations No. 1 of August 1916, which emphasizes 'immediate advance' and 'maintaining the offensive spirit,' using conceptual language characteristic of the classical paradigm. In reality, however, the context of industrialized warfare required a more nuanced approach, based on caution, consolidation, and inter-service cooperation, through coordinated use of infantry, artillery, and cavalry, supported by efficient logistics and communications (NRA, General Headquarters fonds, file 5/1916).

This discrepancy between the traditional offensive doctrine and modern operational realities highlights the Romanian Army's difficulty in adapting strategic planning to a war characterized by prolonged attrition and technical-tactical complexity, anticipating the major challenges of the Transylvanian campaign and the southern front.
This discrepancy between doctrinal language, focused on offense and an aggressive spirit, and operational reality, dominated by enemy resistance and logistical complexity, largely explains the difficulties faced by the Romanian army in the 1916 campaign. Strategic ambitions, supported by the offensive plans developed in August 1916, encountered the concrete limits of mobilization, the insufficient integration of heavy artillery, and the actual reaction capacity of the Central Powers. The result was a rapid transformation of an initially ambitious offensive into a strategic retreat, which required an urgent revision of operational plans and a gradual adaptation of Romanian doctrine to the realities of industrialized warfare.

Romania's 1916 campaign plan still reflected the traditional paradigm of a rapid offensive through Transylvania, designed to achieve a strategic decision through the concentrated and surprising advance of troops. However, this concept underestimated the reaction capability of the Central Powers, as well as the logistical difficulties inherent in a state with limited infrastructure and reduced industrial resources. In practice, theoretical plans quickly confronted the realities of modern warfare: deficiencies in heavy artillery, insufficient ammunition, lack of efficient transportation, and the vulnerability of flanks made it impossible to sustain the initial offensive momentum.

The campaign of 1916 highlighted the structural limits of the Romanian adaptation to industrialized conflict. The planned offensive gradually turned into a crisis defense, characterized by retreats, rapid reorganization of units, and the concentration of effort on defending critical points. Experience showed that, without adequate heavy artillery, stable logistical support, and flank protection, traditional offensive maneuver concepts could not be successfully applied, and Romanian troops were forced to adapt to a war of attrition, in which conserving resources and resilience of the defensive system became strategic priorities.

The gap between doctrine and reality

The period 1912-1916 is marked in the evolution of the Romanian Army by a structural tension between the doctrinal continuity inherited from the 19th century and the profound transformations of modern warfare. Although the Romanian military elites were informed about European doctrinal developments and the lessons of contemporary wars, the effective adaptation of doctrine to operational realities occurred slowly, fragmentarily, and often inconsistently (Popescu 2008, 21–24).

Romania's participation in the Second Balkan War (1913) provided the army with its first experience in a modern, yet limited-intensity, regional conflict. The absence

of major confrontations with a well-equipped opponent led to an overly optimistic perception of the level of preparedness and actual combat capability, which reduced the pressure for profound doctrinal reforms. Consequently, although the reports of the General Staff formally acknowledged the logistical and organizational lessons of the campaign, their implementation was only partial, constrained by material limitations, institutional inertia, and the persistence of an operational culture focused on offensive operations.

The review of the 1915 plans introduced new and relevant elements – concern for the southern flank, recognition of the role of heavy artillery, operational reserves, and cooperation with allies – but these adjustments did not fundamentally change the dominant paradigm. Strategic thinking remained anchored in an offensive-maneuver concept, suitable for the rapid conflicts of the 19th century, but increasingly inadequate for the industrialized war of attrition that was already taking place on the Western and Eastern fronts (MRA, Order of the General Staff No. 22/1915).

This persistence is evident in the campaign plan of August 1916, which provided for a massive offensive in Transylvania, defensively covered by the 3rd Army in the south. The plan reflected a disproportionate confidence in the ability for rapid penetration and in the enemy's weak response, underestimating both the resilience of the Central Powers' defensive systems and the logistical complexity of supporting an offensive on multiple fronts (MRA, Order of the Great General Staff no. 1/1916).

The analysis of the operational orders from the summer and autumn of 1916 confirms this gap. The language used – 'unhindered advance,' 'maintaining the offensive spirit' – belongs to a conceptual universe that favors will, momentum, and initiative, while the reality of war demanded caution, consolidation, inter-service cooperation, and careful management of resources (MRA, Operations Order no. 1/August 1916). Overestimating one's own offensive capability, underestimating the enemy's reaction, and the insufficient integration of heavy artillery and modern means contributed decisively to the vulnerability of the Romanian disposition.

In this regard, the gap between doctrine and reality was not merely technical or logistical, but deeply conceptual: between a military culture built on the paradigm of maneuver warfare and a strategic environment dominated by attrition, industrialization, and the interdependence of arms, economy, and alliances. This discrepancy largely explains the difficulties of the 1916 campaign and the rapid transformation of an ambitious offensive into a strategic retreat (Boia 2010, 120–125).

Although conceptual modernization was visible in official documents and military discourse, the institutional capacity for implementation was limited by structural factors – insufficient infrastructure, a poorly developed military industry, deficiencies in the mobilization system, and an inadequately trained command corps – with the Romanian state being unable to sustain a long-term conflict (Hitchins 1994, 215-230).

Dependence on imports for weapons and ammunition constituted a major strategic vulnerability (Murgescu 2010, 123-140).

After 1918, several Romanian generals published works in which they pointed out the structural deficiencies of the army as early as the 1912–1915 period and emphasized the state's inability to eliminate them before the outbreak of the Great War. Among others, this category includes Generals Alexandru Iarca and Alexandru Averescu, whose analyses highlight both the structural limitations of the army and the tensions between strategic requirements and available economic resources.

In the volume "My Memoir", General Alexandru Iarca offers an interpretation of the state of the Romanian army in the years preceding the war using structural explanations. He shows that deficiencies in armaments, ammunition, and logistical organization cannot be attributed solely to leadership errors but must be related to the economic limits of the Romanian state, characterized by an underdeveloped industry and dependence on imports for military equipment. The experience of the Balkan Wars did not create the army's shortages, but only highlighted them, and the short period before the outbreak of the world conflict did not allow for a substantial correction of these deficiencies (Iarca 1922, 199-232). General Iarca's interpretation shows that, from this perspective, the army's deficiencies arise as the result of a gap between Romania's strategic ambitions and its real economic resources, rather than as the effect of deliberate negligence by political or military leadership.

In the first chapters of the work "Responsibilities," General Alexandru Averescu evaluates the readiness of the Romanian army prior to the 1916 campaign, identifying a series of structural and administrative deficiencies. He emphasizes the insufficiency of modern weaponry, the lack of reserves of ammunition and equipment, as well as the logistical organization, which he considers incompatible with the demands of industrial warfare. In his analysis, these shortcomings are linked to delays in the adoption of equipment programs and to the tendency of the political factor to subordinate the needs of the army to other budgetary priorities. Averescu insists that the experience of the Balkan Wars had already demonstrated the army's vulnerabilities, but the conclusions drawn from them were not sufficiently utilized in the following years (Averescu 1921, 15-42). From this perspective, the 1916 campaign does not appear as the result of a strategic accident, but as an expression of the accumulation of previous deficiencies, caused by the lack of a consistent military policy and the mismatch between strategic ambitions and the available material resources.

Financial assessments made after the war indicate serious structural limits in Romania's budgetary capacity. Thus, in 1922, the Romanian economist and banker of the interwar period, Aristide Blank, pointed out that, to support the military effort, Romania had contracted loans of approximately 1.6 billion gold francs from the British and French governments. This amount becomes all the more significant when compared to the roughly 2.1 billion gold francs needed to modernize the

Romanian state in the half-century preceding the war, funding that came largely from Germany and the Austro-Hungarian Empire. The ratio between these values highlights the disproportion between the state's economic resources and the demands imposed by the world conflict. From this perspective, the criticisms later expressed in the political and memorialist spheres appear insufficiently grounded. For example, General Alexandru Averescu's reproaches regarding the army's inadequate material preparation ignore the real constraints of public finances. The issue was not the diversion of resources or a lack of political will, but rather the modest size of the Romanian state's economic base, which made it impossible to support armament compatible with the standards of the Great War. The costs of such modernization would have exceeded Romania's annual budget in 1914–1915 several times over, which explains the material gaps without resorting to accusations or blame (Cristescu 2019, 23).

Doctrinal modernization was accompanied by institutional resistance driven by professional traditions and the prestige of classical forms of warfare (Huntington 1957, 59–85). This cultural tension limited the pace and depth of change. The period of neutrality was used for doctrinal and organizational adjustments, yet archival documents reveal significant delays in the areas of mobilization and equipment (NRA, Ministry of War records, file 1914-1916).
Thus, the period 1912-1916 can be interpreted not only as a time of military preparation but also as one of latent doctrinal crisis, during which the Romanian Army attempted to transition from a 19th-century war model to the realities of the 20th century - an incomplete transition, rushed by events, and costly, in 1916.

Conclusions

The process of modernizing Romanian military thinking in the period 1912-1916 was real and aimed at becoming integrated into the European trends of the era. However, this modernization remained predominantly conceptual, not being supported by a corresponding institutional and material transformation. The result was an army that 'thought in a modern manner' but still operated within a traditional structural framework.

The Romanian Army entered the war with a modern doctrine, but with an institutional structure that was insufficiently adapted, which explains the initial difficulties in 1916 and the need for subsequent accelerated adaptation. This tension between concept and reality constitutes one of the explanations for the evolution of the Romanian Army in the First World War and provides a useful interpretive framework for understanding the processes of military modernization in small and medium-sized states.

The period 1912-1916 represents a turning point in the evolution of Romanian military thinking, situated between the doctrinal continuity of the 19th century and

the emergence of a new type of war characterized by industrialization, attrition, and systemic interdependence among the situation on the front, economy, and politics. The analysis of doctrinal documents, operational planning, and the conceptual language used by Romanian military elites indicates that the Romanian Army was not isolated from major European debates on the transformation of warfare, but the process of assimilating these debates was fragmentary, selective, and structurally incomplete.

The experience of the Second Balkan War acted as an ambiguous catalyst: on one hand, it provided an initial encounter with a modern type of regional conflict; on the other hand, due to its limited nature, it created a mistaken perception when assessing actual combat capability. This overestimation of one's own effectiveness reduced the pressure for radical doctrinal reforms and favored the maintenance of an offensive-maneuver paradigm in a strategic context that was rapidly becoming incompatible with it.

The doctrinal revisions and successive planning during the 1914-1915 period reflect a gradual awareness of the changing nature of war: explicit references appear to the decisive role of heavy artillery, the importance of operational reserves and logistics, as well as the necessity of cooperation at the allied level. However, these adjustments were more complementary than transformative in nature. They did not alter the conceptual core of the doctrine, which remained centered on the idea of quickly breaking through the front and the primacy of the offensive.

The campaign plan from August 1916 and subsequent operational orders confirmed the persistence of this strategic culture. The normative language of the documents emphasizes will, momentum, and initiative, while the structural dimensions of industrialized warfare – fire density, the resilience of defensive systems, logistical constraints, and strategic timing – are underestimated or treated marginally. This dissonance between doctrinal language and operational reality explains not only the tactical difficulties of the 1916 campaign but also the rapid transformation of an ambitious offensive into a strategic retreat.

Therefore, the modernization of Romanian military thinking in the period 1912-1916 can be characterized not as a failed process, but as one that had begun but remained unfinished, accelerated by the entry into war and later continued under the constraints of front-line realities. This perspective allows for a more nuanced understanding of the evolution of the Romanian Army: not as a result of incompetence, but as an institution undergoing a difficult process of adaptation to a major historical rupture in the way war is conducted.

The modernization of Romanian military thinking between 1912 and 1916 cannot be evaluated in narrow terms of success or failure, but must be understood as a constrained historical structural process, marked by internal tensions and doctrinal contradictions, typical of middle powers caught between imported strategic models and their own institutional limitations. This perspective allows for a reinterpretation

of the Romanian army not as an inert or unworthy institution, but as an actor undergoing a difficult process of adaptation to the fundamental changes brought about by the emergence of industrialized modern warfare.

References

Averescu, Alexandru. 1921. *The Answers*. Bucharest. National Culture Publishing.

Boia, Lucian. 2010. *Romania and the Great War.* Bucharest. Humanitas Publishing.

Buzatu, Gheorghe. 2003. *A History of Romanian Foreign Policy.* Bucharest. Mica Valahie Publishing.

Cristescu, Sorin. 2019. *Considerations on Romania's Participation in the Great War*. București. Military History Magazine, no. 5-6: 21-25.

Delbrück, Hans. 1920. Geschichte der Kriegskunst im Rahmen der politischen Geschichte. Berlin.

Doughty, Robert A. 2005. *Pyrrhic Victory: French Strategy and Operations in the Great War.* Harvard University Press.

Fuller, J.F.C. 1926. The Foundations of the Science of War. London.

Great General Staff. Historical Service. 1934–1946. Romania in World War I: 1916–1919. Documents. vols. I–IV. Bucharest.

___. Training Regulations of the Romanian Army, editions 1912–1915.

Hall, Richard C. 2000. *The Balkan Wars 1912–1913*. Routledge.

Hitchins, Keith. 1994. *Romania 1866–1947*. Oxford University Press.

Howard, Michael. 2009. *War in European History*. Oxford University Press.

Huntington, Samuel P. 1957. *The Soldier and the State*. Harvard University Press.

Iarca, Alexandru. 1922. *My Memorial*. Buzău. Ion Călinescu Publishing House.

Liddell-Hart, B.H. 1941. Strategy: The Indirect Approach. London.

Keegan, John. 1993. A History of Warfare. London.

Murgescu, Bogdan. 2010. *Romania and Europe,* Iași. Polirom Publishing.

Murray, Williamson, Macgregor Knox, Alvin Bernstein. 1994. The Making of Strategy. Cambridge University Press.

Popescu, Alexandru. 2008. *The Romanian Army between Tradition and Modernity (1910–1916).* Bucharest. Military Publishing.

Romanian Military Archives, Revision of the operations plan, 1915, Great General Staff Order no. 22/1915.

Romanian National Military Archives (RNMA), Grand General Staff collection, files 1912–1916.

Strachan, Hew. 2001. The First World War. Oxford University Press.

The National Archives of Romania (NAR), Ministry of War collection, files 1912–1916.

___. Great General Staff collection, file 12/1914, "Instructions on general mobilization".

___. Great General Staff collection, file 45/1914, "Operations plan in case of a conflict with Austria-Hungary".

___. Great General Staff collection, file 33/1915, "Revision of operational plans".

___. General Headquarters collection, file 1/1916, "Campaign plan of the Romanian army," August 1916.

___. General Headquarters collection, file 5/1916, "Operations Order no. 1," August 1916.

Torrey, Glenn E. 1998. Romania and World War I. University Press of Kansas.

Von Clausewitz, Carl. 1982. *On War.* Bucharest. Military Publishing.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Leaders, Personality Traits, and the Foreign Policy Decision Making Process: Theoretical Aspects and Insights from Case-studies

Luqman SAKA, Ph.D.*,* **Lamin JUWARA***
AbdulKareem Jimoh EDUN** **Malang FANNEH***

*Division of Humanities and Social Sciences, School of Arts and Sciences,
University of The Gambia, Faraba Campus, West Coast Region, The Gambia
e-mail: l.saka@utg.edu.gm; https://orcid.org/0000-0002-7811-5268
https://orcid.org/0009-0005-3534-3366 https://orcid.org/0009-0002-1704-2007
**Department of Political Science, Faculty of Social Sciences, University of Ilorin, Nigeria
https://orcid.org/0000-0001-8304-3986

Abstract

Numerous factors influence a state's foreign policy actions and decisions. These factors can be internal to the state (relating to domestic politics) or emanate from the external environment (international politics). Regarding the internal factors, the personality traits of political leaders (notably presidents or prime ministers) remain central in foreign policy analysis, especially from a psychological and behavioural analysis perspective. Understanding leaders' personalities has been deemed to be critical for explaining why they make certain foreign policy choices and decisions. Methodologically anchored on a scoping review of literature and drawing insights from the United Kingdom (UK) foreign policy under Prime Minister Tony Blair, the United States under the George W. Bush presidency, Türkiye under Recep Tayyip Erdogan presidency, and Nigeria under Olusegun Obasanjo and Muhammdu Buhari presidencies, this article discusses how leaders' personalities and behavioural traits shape foreign policy directions of states. This review highlights the continued relevance of leaders' personality traits and the centrality of human agency in a state's foreign policy actions and directions.

Keywords:
Leadership Traits Analysis (LTA); Personality; Foreign Policy Decision-Making; Behavioural Analysis; Human Agency.

Article info
Received: 17 November 2025; Revised: 9 December 2026; Accepted: 21 January 2026; Available online: 8 April 2026

Citation: Saka, L., L. Juwara, A.J. Edun, and M. Fanneh. 2026. "Leaders, Personality Traits, and the Foreign Policy Decision Making Process: Theoretical Aspects and Insights from Case-studies." *Bulletin of "Carol I" National Defence University*, 15(1): 124-144. https://doi.org/10.53477/2284-9378-26-08

Introduction

The conduct of diplomatic relations between and among states is as old as the history of the modern state system (Hudson and Vore 1995, 212). There is documented evidence of relationships between and among European kings and princes, as well as among the Greek city-states. Similar relationships had been recorded among Kingdoms, Chiefdoms, and Principalities in Africa before the advent of colonial rule. This being said, it is important to highlight the fact that the conduct of inter-state relations in the contemporary world has greatly advanced beyond what was usual in the past. Emerging issues, notably the advancement in communication and information technology, have greatly aided the conduct of relations between and among states in the contemporary international system.

Scholars have conceptualized what foreign policy stands for. While there has been variation in conceptualization, a common thread in the discourse is that foreign policy is seen as the behavioural pattern which states adopt in the conduct of foreign and diplomatic relations with other states within the context of global power politics (Bindra 2019, 26-27; Mushtaq and Choydhry 2013, 2). Critical to the country's relations with other states in the international system is the need to preserve and advance certain objectives couched within the discourse of "National Interest". Of course, what constitutes national interest is determined by policy actors, notably the chief executive (presidents and/or prime ministers) and their policy advisers. It is important to note that what constitutes the national interest of a state is dynamic rather than static. It is equally important to note that what constitutes the determinants of a state's foreign policy and the factors that influence foreign policy decisions have also been of significance in the discussion of foreign policy of states in academic literature.

Speaking about issues driving foreign policy, Bindra (2019, 26) noticed that the behaviour of the global community results at least in part from the interactions among the foreign policies of all states whose concrete goals and values are often hard to define as they are influenced by innumerable cultural, economic, geographical, historical, social, and even (irrational) psychological factors. It is also important to affirm that both internal and external factors to the state do influence the foreign policy decisions and/or course of actions that a state's foreign policy actors decide to pursue, either in holistic terms or on a case-by-case basis, as it relates to specific issues in their foreign relations and diplomatic dealings.

Some of the key external factors that have an impact on foreign policy decisions and actions of state's include the following: the politics of the international system, the roles of international organizations, international laws, norms, treaties and agreements that a state willingly signed onto, the activities of multinational corporations, the roles of non-state actors, notably international terrorist groups, criminal networks and insurgents, among others. These factors, which are external

to the domestic socio-economy and politics of a state, do impact the foreign policy direction and course of actions that a state pursues in relations with other states in the international system. Without mincing words, the world beyond national borders significantly impacts foreign policy decisions of states, sometimes forcing states to align national interests with global realities (Marijke 2007, 9).

While factors that are external to the state impose constraints on foreign policy decisions and actions as states largely have to respond to the vagaries of the international system, the domestic environment also has a significant impact on determining the course of actions that the states pursue in their relations with others within the international system. The centrality of domestic factors to the formulation and implementation of foreign policy becomes significant within the context of the position that a state's foreign policy is essentially an extension of its domestic politics (Mushtaq and Choundhry 2013, 12). Issues such as the population size and dynamics, geography, resource endowment, level of economic development and technological advancement, national capability (military strength), culture, values and national history, social structure, power politics and its configuration, the nature of the political system, roles of the press, national ideology and, of course, the world view, perception and orientation of state's political leadership are important internal factors affecting the foreign policy behaviour and/or decisions of a state.

There have been extensive discussions about the roles and impacts of the internal factors influencing state foreign policy decisions and actions in foreign policy literature. There have also been extensive discussions on the roles of political leaders (Presidents and Prime Ministers) as key internal factors that shape the foreign policy directions of states. The discourse on leadership and foreign policy making has been re-energized within the context of emergent discussion in the sub-field of political psychology (Thiers 2025; Suresh 2022, 9; Houghton 2017; Puscas and Ciot 2012, 53; Greenstein 1992, 106-107). The perception and belief of a state's leader about the nature of the international system, the interest that ought to be pursued by the state, the intellectual strength and weakness of the leader, especially as it relates to the analysis of information for foreign policy decision making, life background, emotional stability, among other personality traits of the Chief executive (presidents and/or prime minister) can exert significant influence on foreign policy directions of state. While there is no denying the fact that governmental and social structures constrain the role of leaders in the formulation and execution of their state's foreign policy, idiosyncratic qualities and/or traits of leaders play a significant role in determining the foreign policy formulation and execution, especially as it relates to foreign policy directions and objectives.

While emphasis on the need to understand leaders as individuals is not new, in the context of rising geopolitical tensions and disruptions characterising international politics of recent times, understanding leaders' personality, beliefs, and worldview is no longer a luxury but rather a necessity (Thiers 2025). Thus, the need to continually

re-examine the centrality of leadership personality traits and the influence they exert on a state's foreign policy formulation and execution is, by all means, more important now than before.

To this end, utilizing data from a scoping review of literature and drawing insights from case studies, this article contributes to the discourse on personality in decision-making by re-examining the centrality of leadership personality theory in the formulation and execution of foreign policy. Following this introduction, the article discusses personality, politics, and the foreign policy decision-making process, underscoring the strong impact of personality traits on a leader's worldview and foreign policy outlook. The next section of the article draws insights from various cases to show how the personalities of leaders shape the nature and dynamics of nations' foreign policy, using as examples Britain under Prime Minister Tony Blair, the United States of America under the presidency of George W. Bush, Türkiye under the Recep Tayyip Erdogan presidency and Nigeria under the Olusegun Obasanjo and Muhammadu Buhari's presidencies. Using these countries and leaders, the article demonstrates how leaders' personalities and behavioural traits influence state foreign policy actions and directions.

Personality, Politics, and Foreign Policy Decision Making

Understanding human psychology is crucial for grasping how political leaders and policymakers as individuals navigate the complex web of policy process, especially in the realm of foreign policy and diplomatic relations. Indeed, it is important and a worthwhile venture to engage in analysing how individuals' leadership traits influence the policy decisions of states. To this end, one of the primary objectives of the sub-field of political psychology is the application of insights relating to human cognition and personality to study the centrality of political leaders in the policy-making process and how leaders' perception, worldview, and other personality traits shape the course of actions they take on behalf of their states. While studies on political psychology, including leadership traits analysis of individual political leaders and policy makers, signal inherent challenges, nonetheless, progress has been made in the subfield of behavioural analysis and policy process. Integrating behavioural analysis (leadership traits analysis) into discourse on leaders' decision-making is essential as this approach aids scholars to understand how the worldview, beliefs and leadership style of political leaders influence their policy choice, decisions, and courses of action in the domains of domestic and international politics (Levy 2023, 350; Dyson 2006, 290-291; Hermann 2005, 178-179; Schafer 2000, 511).

Understanding leadership disposition and personality traits' influence on political decisions is crucial. This is because political institutions and processes operate through human agency. Thus, it would be difficult to assert that the process of arriving at a policy decision is not in any way influenced by human agency. Underlying the centrality of human agency in the political decision- making process, Greenstein (1992, 105)

notes that "personalities of political actors impinge on political affairs in countless ways, often with great consequences". Drawing from the above position, Renshon and Renshon (2008, 511) note that, "while system level variables aid the efforts at explaining or predicting broad historical trends, no crisis or war is understandable without direct reference to the decision making of individual leaders". The handling of the 'Cuban Missile Crisis' of 1962 was highly influenced by the psychological disposition and personality traits of the late President John F. Kennedy.

This, in essence, affirms the centrality of political leaders to the making of critical foreign policy decisions, especially those that deal with the initiation of wars and policy directions in conflict resolution. As human agency, the personality of leaders greatly impacts the courses of action that states pursue in their relationships with other states within the international system. Indeed, the general assumption within the broad field of international relations is that foreign policy crises and wars involve conditions which favour the influence of personality, and that individuals' distinctive policy preferences, decision making styles, and relationships to advisers are crucial elements in accounting for policy positions and outcomes (Galea 2022; Dyson 2006, 290; Winter 2003, 112; Preston and 't Hart 1999; Preston 1997). To this end, Dev and Arli (2025, 1-2) further stressed that "personal attributes influence how actors, whether students making career choices or political leaders making foreign policy decisions, interpret information, cope with uncertainty and choose among competing options". Understanding the psychological foundations is essential for explaining variation in behaviour, whether in foreign policy, leadership evolution, or decision-making under pressure.

Commenting on the centrality of the human agency in international relations, Hudson and Vore (1995, 209) note that students coming of age in the post-Cold War period intuitively grasp the notion that the study of International Relations is ultimately about human beings, and that the ways in which human beings engage in such relations on behalf of the state as the most significant actors in inter-state relations is difficult to simplify. In order to provide adequate explanations and offer predictions about states' behaviour in international politics, International Relations requires a theory of human political choice (Gaddis 1992/1993, 6). A sub-discipline of International Relations that has engaged in an attempt to develop a theoretical perspective that gives primacy to human agency in International Politics is foreign policy analysis. According to Hudson and Vore (1995, 210), foreign policy analysis, from its inception as a sub-discipline of international relations, has engaged in the examination of how foreign policy decisions are made and has assumed that the source of much behaviour and most changes in international politics are attributable to human beings, acting as individuals or in groups.

Without doubt, certain systemic issues, such as the Cold War bipolar system, may somewhat constrain the importance of human actors, yet it becomes apparent with every system transformation that human will and imagination are major influences

shaping world affairs (Hudson and Vore 1995, 210). Arising from this, it can be argued that the major events that have shaped the configuration of international politics such as the September 11, 2001 terrorist attacks and subsequent reactions that accompanied it, especially from the United States are highly determined by the personality of the major political actors that were involved in formulation of US foreign policy, notably then President George W. Bush and Secretary of State Dick Cheney. The proactive position of former President Olusegun Obasanjo over the military coup and ensuing crisis in Sao Tome and Principe and the closure of Nigeria's borders with the Benin Republic in 2003 were largely shaped by the personality traits of then-President Obasanjo, his views on what Nigeria's role in Africa's affairs was supposed to be, and his demonstrated interest in foreign policy.

The importance that should be attached to personality traits of political leaders as it relates to the making of foreign policy was acknowledged by former US Secretary of State, Henry Kissinger when he was quoted to have stated that "As a professor, I tended to think of history as run by impersonal forces. But when you see it in practice, you see the differences personalities make" (Byman and Pollack 2001 cited in Kesgin 2012, 29). Kissinger's statement reifies the long-held position of scholars of foreign policy that the individual constitutes the heart of international politics (Hudson 2005, 1-3). Indeed, for scholars who follow in the footsteps of Snyder, Bruck, and Sapin, political leaders' individual personality traits influence state behaviour in a significant manner (Snyder, Bruck, and Sapin 1962 cited in Kesgin 2012, 29). Thus, personality traits "beliefs, motives, decision-making style, and interpersonal style) affect personal orientation to behaviour, which in turn shapes a leader's general orientation to foreign affairs" (Hermann 1980, 12, cited in Kesgin 2012, 29). Arising from this, it is then clear that a leader's orientation towards foreign affairs gives information on the kind of policy choice they will make on behalf of the state. In essence, "individuals or groups of individuals are the sources of all state actions" (Kesgin 2012, 29) and ultimate makers of state foreign policy decisions (Kesgin 2012, 29; Hudson 2005, 3). In an article titled, "Who makes foreign policy decisions and how", Hermann and Hermann (1989, 384) note that, "at the apex of foreign policy making in all governments or ruling parties are actors with the ability to commit resources of the state and the power to prevent other entities within the government from reversing their position". They characterized such actors as the "ultimate decision unit". To them, the ultimate decision-making units, be it a predominant leader, single group, or multiple autonomous actors, hold a strong influence in determining the foreign policy direction of the state or the particular line of action as it relates to a specific issue of international concern. While they agree that internal and external pressures may predispose a government to act in a particular manner, they argued that "the precise character of state actions will be modified by properties of the ultimate decision unit" (Hermann and Hermann 1989, 384). In essence, the personality traits of the human agency working through the medium of the ultimate decision unit in all three units of analysis that they identified are central to the determination of the foreign policy decisions and actions of the state (Hermann and Hermann 1989, 384).

In an earlier work, Hermann, Margaret G. (1980a) had noted that debates concerning whether the personal characteristics of political leaders could have effects on policy decisions had been conducted more in the sub-discipline of foreign policy. Studies including Crow and Noel (1977), Driver (1977), Falkowski (1978), Hermann (1974, 1977), and Winter and Stewart (1977) showcase portraits of national political leaders who influence their governments either towards an aggressive or conciliatory relationship with other states. Hermann (1980a, 7-8) notes that data from previous studies mentioned above suggest that aggressive leaders are high in need for power, low in conceptual complexity, distrustful of others, nationalistic, and likely to believe that they have some control over the events in which they are involved. In contrast, conciliatory leaders are high in need for affiliation, high in conceptual complexity, trusting of others, low in nationalism, and likely to exhibit little belief in their own ability to control the events in which they are involved. All the leaders' portraits that the studies tried to build are inferred from the personal idiosyncratic qualities of political leaders. Personality traits aid in the drawing up of four types of personal characteristics, which are *beliefs, motives, decision style,* and *interpersonal style*. Hermann, (1980a, 8) notes that these four personal characteristics strongly impacted the content and means of making political decisions by national political leaders. Thus, there is no controversy regarding the position that leaders' idiosyncratic traits have a strong controlling influence on foreign policy decisions taken in the name of the state.

The position advanced by Hermann (1980a, 12) in the study is that the personal characteristics of leaders that were the focus of the study interrelate to form a personal orientation to behaviour or a general way of responding to one's policy environment. The personal orientation is transformed by the head of government (presidents or prime ministers) into a general orientation to foreign affairs and international politics. Knowing a head of government's orientation to foreign affairs helps in predicting their predispositions and course of action when faced with a foreign policy-making task. This is because the leader's orientation will influence how he/she defines the situation and the style of behaviour he/she is likely to emphasize. Heads of government with the personal characteristics discussed in Hermann's study (1980a) are thought to be predisposed toward either an independent or participatory orientation to foreign affairs, depending on how the characteristics interrelate. Thus, leaders who portray aggressive behavioural traits are more predisposed to assert independence in foreign policy orientation and decision-making, while those who portray conciliatory traits are more likely to engage in participatory foreign policy decision-making (Hermann 1980a, 12-13).

The portraits of national leaders referred to by Hermann (1980a) represent, by far, a pioneering work in the psychological analysis of leaders' personality traits and their implications for foreign policy decision-making. The study was an offshoot of what now becomes 'Leadership Traits Analysis' (LTA), an approach that has been extensively deployed in studies that assess the impacts of leaders' traits on a state's foreign policy (Niek 2014; Kesgin 2012; Dyson 2006; Hermann 1980b, 2002; 2005).

Leadership trait analysis developed by Hermann (1980a, 1980b, 2002, 2005) is an attempt to assess leaders' personal styles based on content analysis of written or spoken words available in public domains (Niek 2014; Kesin 2012).

"At-a-distance" techniques designed to overcome the problem of access in the conduct of analytical research on important political figures are the process of profiling political leaders based on their publicly available verbal records (speeches, interviews, letters, memoirs, among others). The methods entail meticulous designed procedure of coding and operationalization of selected personality measures and an adaptation of conventional psychological personality measurements deployed for studying leaders' behavioural traits and how it influences their foreign policy decision-making (Hermann 1980b; Winter 1992; 2003; Schafer 2000).

As Young and Schafer (1998, 63-64) note, "LTA is a significant research agenda that seeks to measure leaders' cognition and its implications for foreign policy decision-making process". The techniques advance the position that leaders' choices of certain words reflect their personalities (Kesgin 2012, 32). As a methodological approach to studying the implications of personality traits for leaders' foreign policy decisions, LTA entails a careful content analysis of leaders' discourse and quantifying it into seven traits. These traits are: the belief that one can influence or control what happens; the need for power and influence; conceptual complexity (the ability to differentiate things and people in one's environment); self-confidence; the tendency to focus on problem solving and accomplishing something versus maintenance of the group and dealing with others' ideas and sensitivities; general distrust or suspiciousness of others; and the intensity with which a person holds an in-group bias (Kesgin 2012, 32; Dyson 2006, 292; Hermann 1980a; 1980b; 2002; 2005). By measuring the score that a particular leader earns in each of the traits, proponents of the techniques argued that one will be able to determine the disposition of the leader's foreign policy decisions on important issues as they arise (Kesgin 2012; Dyson 2009a; 2009b; 2006; Dyson and Billordo 2004; Hermann 2003). These studies, among others, illustrate the importance of leadership traits analysis as a method for explaining foreign policy behaviour and linking this behaviour with the personalities of decision makers (Kesgin 2012, 36).

Recent empirical investigation has extended the application of personality psychology to foreign policy decision-making during global crises, offering a critical bridge between individual traits and transnational policy coordination. Medeiros, Nai. Erman and Young (2022, 1-2) studied the leaders' personality attributes in 61 countries as part of a broad study on government response patterns during the COVID-19 pandemic, relying on the NEGex expert surveys and focusing on leaders' meta-factors of *plasticity* (covering extraversion and openness) and *stability* (covering conscientiousness, agreeableness, and emotional stability). Using data from the Oxford COVID-19 Government Response Tracker, the authors used regression models to show that, especially in centralized political systems, leaders with a high level of plasticity enacted stronger responses and implemented relief and travel restrictions more quickly. Conversely, leaders with high stability prioritized

rapid fiscal stimulus, reflecting a preference for group maintenance and procedural certainty. The findings illuminate how personality moderates the speed and scope of crisis response, even under systemic pressures such as GDP and infection rates. While focused on domestic policy outputs, the study's implications for foreign policy are profound: border closures, vaccine diplomacy, and multilateral aid coordination, all core foreign policy instruments, were shaped by leaders' cognitive and affective dispositions (Medeiros et al. 2022, 8-9).

While appreciable progress has been recorded in the academic study of the individual role in shaping foreign policy behaviour and decisions of the state, reservations continue to be expressed about the utility of studying the personalities of political actors on a number of grounds. The first criticism is that political actors are randomly distributed in roles and therefore their personalities are cancelled out by those of others. There is also the argument that political action is determined more by the political actors' operating environments than by their own characteristics. Critics have also advanced the position that the social characteristics of political actors are more important than their psychological characteristics (Borna and Randy 2023; Judge, Piccolo, and Kosalka 2009; Zaccaro 2007). It has also been argued that individuals are typically unable to have much effect on political outcomes, contrary to the position of studies that have sought to give significance to leaders' personality traits as important variables in explaining foreign policy decisions (Greenstein 1992, 106-107).

Aside from the above, the LTA methodology that has been used to profile personality traits of many notable political leaders and the impact on their states' foreign policy directions and actions have also been subject to criticisms. For instance, LTA has been criticized for its inability to capture the leader's personality. Instead, it was argued that the methodology at best provides a snapshot of a leader's personality at a certain moment. Responding to the criticism, Hermann (1980b) makes it clear that personality can be contextually dependent, and this can be determined by studying diverse materials. Notwithstanding the criticisms, levied at LTA, Hermann (2003) notes that it is still widely acknowledged that many leaders' profiles that were assessed using the methodology correspond with the image of those leaders in the eyes of other leaders, their advisers, public commentators and analysts, as well as political journalists. Thus, criticism notwithstanding, the academic study of foreign policy has and will continue to benefit much from research and studies that focus on the roles of individual political actors and how their personality traits shape the foreign policy decisions they make on behalf of the state.

Leadership Traits and the Making of Foreign Policy Decisions: Insights from Case Studies

Leaders can be found across professions in society; thus, leadership and issues surrounding it have been the focus of study in many academic disciplines. In politics, leaders occupy positions of prominence as heads of state or governments. The power

invested in their political offices and personality dispositions can make a significant difference in galvanizing the growth of business and economic development. Political leaders can push the frontier of knowledge through investment in education and technological acquisition. Moreover, political leaders have used their charisma to cheer their sports teams to victory in crucial sporting tournaments, as demonstrated by President Mandela's crucial message to the Springboks during the 1996 Rugby World Cup.

In the field of politics and foreign relations, the character of national political leaders becomes an important intervening variable in decision-making, especially in crisis situations and notably on issues of conflict and war. While internal and external variables act as factors constraining foreign policy decisions that states adopt, the centrality of leaders' personality and traits as an important factor in the making of foreign policy decisions cannot be undermined. Studies including Kesgin (2012), Dyson (2006; 2009a), Hermann (1974, 1977, 1980a, 2002, 2005) have demonstrated the importance of political leaders' personality in the attempt to understand foreign policy decisions taken on behalf of the state on an issue and to predict what actions a leader will take on issues of importance in the future (Breuning 2007, 33).

It has often been posited that leaders' experience over time results in the development of stable patterns of choice, as well as a constant outlook on the nature, patterns, and operation of the international system. This brings into discussion issues of character psychology, strategic worldview, and operational codes. Thus, leaders must also confront, to some degree, the complexities of the real circumstances that they face. Leaders also need to juxtapose these realities with hosts of other matters, including the views and intentions of adversaries and friends that they engage with, the histories of the issues they intend to address, the range of options available to them, and the implications of each course of action and/or decision. In essence, leaders operate in the context of information, and it is important that they gather and process data with the objective of arriving at decisions and courses of action that fit both the facts available to them and the political and strategic realities that face their nations. How a leader gathers such information, how this is framed and understood, the cognitive aids that are used in so doing, and their accuracy and effectiveness profoundly affect the course of world politics (Renshon and Renshon 2008, 510).

Studies have approached cognition, psychology, and personality traits of leaders and used them as yardsticks to analyse foreign policy positions, decisions, and courses of action they take on important international issues. As demonstrated in the previous section of this article, a number of influential studies have been conducted on leadership personality, characteristics, and behavioural traits, and how these impact foreign policy decisions of states. There have been single-leader, single-issue studies on United States presidents and the foreign policy decision-making process on critical issues of war and peace. Studies have also been conducted on the personality traits of political leaders from Europe and how

these traits and personal attributes shaped the nature and course of foreign policy directions of states under their regimes.

In a comparative study on prime minister leadership styles and foreign policy decision making, Kaarbo (1997, 553) notes that prime ministers exhibit variation in their leadership styles, especially as it relates to leaders' work habits, how they relate to those around them, how they like to receive information, and how they make up their mind on important foreign policy issues. Kaarbo (1997) argued that the differences exhibited by prime ministers in the discharge of the duties of their offices are not trivial. Indeed, Kaarbo (1997) averred that prime ministers' leadership styles can influence the foreign policy of parliamentary democracies.

While there is a noticeable difference in the structure of power and decision process between presidential and parliamentary system, however, just as with presidents, there are systematic ways in which prime ministers' leadership styles differ within similar political constraints. These differences in leadership style can have both direct and indirect effects on foreign policy. The primary mechanism through which a prime minister's leadership style affects foreign policy is the decision-making process. Prime ministers can shape the decision-making process in a number of ways. They can establish subcommittees or inter-ministerial consultation groups, absent themselves from important meetings, make decisions on their own, allow issues to be placed on cabinet agendas, and block the moving of a decision from an inner cabinet to a full cabinet. This process, in turn, shapes the final foreign policy decision (Kaarbo 1997, 554). In summary, Kaarbo (1997, 560) notes that individuals and their personality traits are important under certain conditions, and that the study of the characteristics of a prime minister's leadership style can add to our understanding of policy (foreign) decision-making processes and outcomes in parliamentary systems. Kaarbo (2020) further explains that while a leader's personality influences foreign policy, leaders do not stay psychologically static and often change in troubling ways. Often, as leaders remain in power, instead of consistently improving through experience, many grow more authoritarian, overconfident, insulated, and less complex in their thinking. Kaarbo (2020) further argues that the effect of aging, accumulated power, and prolonged authority can distort judgment and increase the likelihood of poor foreign policy decisions.

To highlight how a leader's traits, personality, and worldview shape the foreign policy actions, decisions, and directions of states, this article draws insights from the United Kingdom under Prime Minister Tony Blair, the United States under President George W. Bush, Türkiye under President Recep Tayyip Erdoğan, and Nigeria under Presidents Olusegun Obasanjo and Muhammadu Buhari. The first two choices were anchored on the need to understand how these leaders' personality and traits shaped their decisions to initiate the 2003 invasion of Iraq against strong objection from key members of the United Nations Security Council. The choice of Türkiye was determined by the way President Erdogan's personality led to the transformation of its foreign policy to an assertive, transactional, and independent one, positioning the country as an influential *Middle Power*. And, last but not least, the argument for

choosing the two Nigerian leaders was to show how personality differences between them manifested in foreign policy actions, postures, statements, and how these ultimately shaped the country's foreign policy directions.

In assessing UK foreign policy under Tony Blair (1997-2007) and the interventionist role he pushed Britain to take on, the crises that he tackled as Prime Minister, Dyson (2009c, 2006) argues that Blair was never likely to keep Britain out of Iraq. This is because his personality and worldview, as demonstrated in the pre-Iraq wars he fought, show his predisposition to an interventionist agenda, should there be the need for a military invasion of Iraq. Dyson (2007, 2006) notes that Blair has a distinctive worldview and leadership style, and that these shaped the nature of British foreign policy in Blair's years, especially as it relates to the country's foreign policy direction in the Kosovo crisis, the September 11, 2001, terrorist attack in the United States, and the 2003 invasion of Iraq. Thus, if another person had been prime minister, the foreign policy issues of that decade would have been dealt with differently (Dyson 2009c, 236-237). In essence, the personality of Blair, his worldview, and belief in his ability to influence the course of events all came out to play in the foreign policy directions he pursued as Prime Minister. The argument was that Blair's personality traits are influential in explaining the interventionist role he made Britain play in Kosovo, the invasion of Afghanistan after the September 11, 2001, terrorist attack, and the 2003 invasion of Iraq (Dyson 2009c, 2006).

Using the response in the aftermath of the September 11, 2001, terrorist attacks, notably the invasion of Afghanistan and Iraq as a point of reference, Pfiffner (2004) notes that President George W. Bush demonstrated an impressive display of political leadership. Through his leadership quality, President Bush was able to overcome the skepticism of the professional military in the US, the opposition of much of the world, and the lack of support from the UN Security Council to take the United States to war with Iraq in order to depose Saddam Hussein. Over the crisis period spanning the time immediately after the September 11, 2001, terrorist attack till the deposing of Saddam, President Bush exhibited several patterns of behaviour that provide some insight into his policy choices. Pfiffner (2004: 161) says that "President Bush showed a preference for moral certainty over strategic calculation, tendency for visceral reaction rather than reflection, preference for clarity rather than complexity, a bias toward action rather than deliberation, and a preference for the personal over the structural or procedural". President Bush exuded confidence and moral certainty and exhibited no evidence of self-doubt or ambivalence about major decisions (Pfiffner 2004, 161). While recognizing the fact that many presidential options are constrained by the established structure of the office and by environmental demands on the president, Pfiffner (2004, 161) argued that the Bush presidency illustrates the impact of personality on the major policies of a presidency.

Pfiffner (2004, 176) notes that the presidential personality makes a difference in an administration's policy priorities and achievements, irrespective of environmental and

structural constraints on the office. Deriving from this, President George W. Bush's personality as exhibited in his bias for action, his moral certainty, and his personalistic approach to politics has made important differences in his policy choices and thus in the direction of the United States foreign policy during his reign. President Bush's bias for action led to his early decisions about war in Iraq, his willingness to use factually incorrect documents to argue for it, and his decisions to begin the war with a "rolling start". The President's moral certainty, based in part on religious beliefs, led to his conviction that God had chosen the United States to "extend" universal values throughout the world, sometimes through war. His personalistic approach to politics led to easing relations with Russia and aggravating relations with North Korea. The manifestations of the traits inherent in President G.W. Bush can confer advantages or prove detrimental to the conduct of foreign policy, as with the personality traits of other notable national leaders (Pfiffner 2004, 176).

While studies on personality and foreign policy have focused more on United States presidents and leaders in Western Europe, as well as Russia, there have been reports that have sought to assess the impact of personality traits of leaders of emerging economies on their nation's foreign policy directions. Utilizing the LTA methodological approach, Kesgin (2012) studies the leadership traits of Turkish female Prime Minister Tansu Çiller (1993-1996) that led Türkiye through the turbulence that characterized the period immediately after the Cold War. Drawing insights from the results of Ciller's LTA, Kesgin (2012, 31) concludes that, compared to other Turkish prime ministers since the 1990s, Çiller lacked self-confidence, had a high distrust of others, and a high in-group bias. These traits are reflected in her radical proposals to deal with various complex issues during her mandate. Of significance is the disposition to send troops to the contested Mediterranean islet of Kardak at the height of tensions with Greece and the proposal to bomb "suspected" terrorist camps in Iran. During the Kardak crisis, Çiller was noted to have averred that "This is our legacy: We do not give away territory. We do not concede even an inch of territory or a pebble. We can sacrifice lives, but not pebbles..." (Kesgin 2012, 42).

Studies have also used the LTA methodological approach to analyse how Mr. Recep Tayyip Erdogan's personality traits have shaped Türkiye's foreign policy over more than two decades of his leadership, first as Prime Minister (2003-2014) and then as president (2014 to date) (Balci and Efe 2021; Kutlu et al. 2021; Gorener and Ucal 2011). For instance, using LTA, Gorener and Ucal (2011) performed an analysis to assess the influence of personality traits of President Recep Tayyip Erdogan on Turkish foreign policy actions and directions. The authors noted that Erdogan is by any standard the most controversial and enigmatic political leader in recent Turkish history (Gorener and Ucal 2011, 357-359). Given the preponderance of Erdogan's influence and control over the political structure and institutions in Türkiye, they averred that any attempt to explain Türkiye's recent foreign policy outcomes will be seriously lacking in merit without a thorough consideration given to Erdogan's leadership impact. Flowing from Gorener and Ucal's (2011, 375) analysis of Erdogan's personality traits, the authors

note that he portrays an "evangelist" orientation to politics. This style results from a combination of the tendency to challenge constraints in the environment, closedness to information, and having a relationship focus.

Gorener and Ucal (2011, 376) note that Erdogan's leadership style impinges upon Türkiye's most controversial foreign policy position that departs from the established line. Erdogan's personality traits and leadership style, without doubt, significantly impacted contemporary Türkiye's foreign policy decisions as it relates to the relationship with the European Union, the United States, the civil war in Syria, the clash with Russia and later rapprochement, on Iran and the nuclear issue, on Armenia and Greece, and the persistent Kurdish questions in the region. Gorener and Ucal (2011, 377) aver that while the conceptual framework of Turkish foreign policy was originally placed on a solid foundation in AKP's led government, the day-to-day working of this scheme has been captive to snap judgments, emotional rhetoric, and idiosyncratic preferences of its leader, Recep Tayyip Erdogan". Thus, discussing recent Turkish foreign policy without adequate consideration given to the influence of Erdogan will be but an incomplete and fruitless discussion.

Deploying the LTA methodological approach, Balci and Efe (2021) examine how exogenous variables lead to changes in the personality traits of the Turkish President. The central thesis of their study is to determine whether leadership attributes change or persist over time and experience in office, and after a traumatic event. Justifying their choice, Balci and Efe (2021, 150) argued that Erdogan provides an excellent case for a study aimed at measuring the effect of experience in office and traumatic events on a leader's personality attributes. Their findings suggest that exogenous dynamics, traumatic events, and tenure in office have a significant effect on a leader's traits (Balci and Efe 2021, 161). Thus, instead of explaining policy change by comparing leaders in power with their predecessors, Balci and Efe argue that personality shifts in a specific leader can lead to varying analytical implications (Balci and Efe 2021, 161). In the case of Erdogan, findings prove that using the average scores of political leaders who stay in office for a long period of time and experience traumatic events can be misleading. Thus, instead of conceiving traits as situation-free, LTA scholars should allow for the effects of experience and traumatic events as exogenous dynamics alongside role change (Balci and Efe 2021, 162). The conclusions from the quoted study constitute a call for re-examining the methodological approaches in doing LTA.

The global surge of populist leadership has introduced a distinct foreign policy style, characterized by anti-pluralism and personalistic decision-making, as revealed through LTA. Thiers and Wehner (2022) profiled Hugo Chavez and Donald Trump using Hermann's (2005) seven-trait model, coding public speeches via automated content analysis. Both leaders scored exceptionally high on distrust in others and in-group bias, with low conceptual complexity, fostering a Manichean "people versus elite" worldview. These traits translated into confrontational foreign policies:

Chavez anti-imperialist coalitions (e.g., Bolivarian Alliance for the Peoples of Our America (ALBA) founded in 2004 to serve as counter-balance alliance to US led alliance and coalition in Latin America) and Trump's unilateral withdrawals (e.g., Paris Agreement) signifying a deviation from global leader norms were significant, indicating that populist ideology amplifies aggressive LTA profiles. While structural variables (e.g., oil dependence, party system) moderated outcomes, personality remained the primary driver of foreign policy style (Thiers and Wehner 2022, 5-9).

Although Ojieh (2016, 203) makes a case for the consideration of extraneous variables that shaped leadership's behaviour and implications for foreign policy with reference to Nigeria, he did acknowledge the roles of leadership personality as an intervening variable in explaining Nigeria's foreign policy decisions. There are several studies that have assessed the influence of leaders' personalities on Nigeria's foreign policy actions and directions. Notable among these is Ogwu (1986) study on the country's leaders between the first and second republics. Ogwu (1986, 52) notes that Prime Minister Tafawa Balewa was calmer and more moderate, his personality being more calculated to placate than to provoke, and as such Balewa's positions on foreign policy were marked by conservative and moralistic gradualism. Thus, Balewa's personality traits shaped the state's relations with Britain and the West, the handling of Equatorial Guinea's mistreatment of Nigeria's migrant workers, its position on the establishment of the Organization of African Unity, and relations with Apartheid South Africa (Olusanya and Akindele 1986, 3).

On the contrary, individual assertiveness, the belief that one can influence the environment and persuade others were noticeable personality traits of General Murtala Muhammad and they largely made informed decision such as the unilateral recognition of the Popular Movement for the Liberation of Angola (MPLA) and other policy decisions on Angola, the resolution of the Zimbabwe independence issue and on Apartheid in South Africa (Fawole 2003; Garba 1987, 18-19). For General Muhammadu Buhari, the traits of personal convictions, strong will, and unyielding personality are important, valid bases for explaining Nigeria's foreign policy under his regime as Military Head of State, with the tit for tat attitude that characterizes the handling of Umaru Dikko kidnapping saga as case in point (Ojieh 2016, 2009; Fawole 2003, 14-16). President Olusegun Obasanjo's second term as a civilian president was reminiscent of his first stint as military Head of State. Ojieh (2016) notes that Obasanjo was resolute in his word; this was demonstrated in his decision to enter into a prejudgment agreement to abide by the decision of the International Court of Justice (ICJ) on the disputed Bakassi Peninsula. President Obasanjo also demonstrated strong will and the penchant to take unilateral actions even as a democratic president. These traits were demonstrated in his decision to abide by the ICJ rulings and the granting of asylum to President Charles Taylor of Liberia, both against public opinion and without much consultation with the Nigerian parliament and other foreign policy decision-making institutions (Ojieh 2008, 87). As a democratically elected president, Muhammadu Buhari (2015-2023)

demonstrated bluntness, strong will, and a lack of tact in the management of Nigeria's foreign policy. These personality traits were visible in President Buhari's statements on foreign policy. His personality traits profoundly impacted the country's foreign image and shaped its foreign policy directions, diplomatic engagements, and courses of action in his eight years of rule in his second stint as a democratically elected president (Saliu 2016; Samson 2015).

Conclusion

The specialized literature in the sub-discipline of foreign policy analysis shows that increasing attention has been devoted to the examination of the role that individual, notable political leaders play in the determination of the foreign policy directions of their states. Across the three levels of analysis in foreign policy (individual, national/state, and international system), the role of the individual in determining the nature and dynamics of international politics and the course of global events cannot be underestimated. As studies have affirmed, explanations of many important historical events give considerable causal weight to the role of individual political leaders and the way their psychological and personality traits influence the decisions they take on behalf of the state. To this end, understanding leaders' personalities is essential for explaining why they make certain foreign policy choices; thus, personality-based analyses help to deepen our understanding of past decisions and may even offer some ability to anticipate how specific leaders are likely to behave.

Hardly can there be a meaningful discussion of the Second World War and the Holocaust without reference to Adolf Hitler. In the same vein, explaining the United States wars in Afghanistan and Iraq will not be complete without a critical assessment of the personality of President George W. Bush and, of course, his ally across the Atlantic, Prime Minister Tony Blair. Discussion of contemporary Russian politics and foreign policy without an assessment of the influence of the personality traits of President Vladimir Putin will result only in a partial analysis. The same can be said of Türkiye without Erdogan, South Africa without President Tambo Mbeki, and Nigeria without President Olusegun Obasanjo. These, among other prominent examples, have led some International Relations scholars to acknowledge that "who leads matters" and to reify the important role of psychological variables in foreign policy decision-making.

References

Balci, Ali, and Ibrahim Efe. 2021. "Exogenous Dynamics and Leadership Traits: A Study of Change in the Personality Traits of Recep Tayyip Erdoğan." *All Azimuth: A Journal of Foreign Policy and Peace* 10 (2): 149-164. DOI:10.20991/allazimuth.956105.

Bindra, S. Sukhwant. 2019. "Analysing Foreign Policy: A Theoretical Perspective." *World Affairs: The Journal of International* 23 (3): 26-43. https://www.jstor.org/stable/48531048.

Borna Jalsenjak, and L. Richards Randy. 2023. "Traits and Behavior Theory of Leadership: Critique from Un distributed Middle." *Journal of Leadership Studies* 17 (3): 28-35. https://doi.org/10.1002/jls.21862.

Breuning, Marijke. 2007. *Foreign Policy Analysis: A Comparative Introduction.* 1st Edition. Basingstoke: Palgrave Macmillan. https://link.springer.com/book/10.1057/9780230609242.

Byman, Daniel, and Kenneth M Pollack. 2001. "Let us now Praise Great Men: Bringing the Statesman Back" *International Security* 25 (4): 107-146. https://doi.org/10.1162/01622880151091916.

Crow, J. Wayman, and Robert C. Noel. 1977. "An Experiment in Simulated Historical Decision Making." In *A Psychological Examination of Political Leaders*, edited by Margaret, G. Hermann, 385-405. New York: Free Press.

Dev, A. Mine, and Nuran B Arli. 2025. "The Role of Personality Traits and Decision-Making Styles in Career Decision-Making Difficulties." *Behavioural Sciences* 15 (2), 159. https://www.mdpi.com/2076-328X/15/2/159.

Driver, J. Michael. 1977. "Individual Differences as Determinants of Aggression in the Internation Simulation." In *A Psychological Examination of Political Leaders* edited by Margaret G. Hermann, 337-353. New York: Free Press.

Dyson, B. Stephen. 2006. "Personality and foreign policy: Tony Blair's Iraq decisions." *Foreign Policy Analysis* 2: 289-306. https://doi.org/10.1111/j.1743-8594.2006.00031.x.

___. 2009a. *The Blair Identity: Leadership and Foreign Policy*. 1st edition. Manchester and New York: Manchester University Press.

___. 2009b. "Stuff Happens": Donald Rumsfeld and the Iraq War." Foreign Policy Analysis 5 (4): 327-347. https://doi.org/10.1111/j.1743-8594.2009.00096.x.

___. 2009c. "What Difference Did He Make? Tony Blair and British Foreign Policy from 1997-2007." In *The Blair Legacy*, 235-246. London: Palgrave Macmillan. https://doi.org/10.1057/9780230232846_17.

Dyson, B. Stephen, and Lorena L Billordo. 2004. "Using Words as Data in the Study of The French Political Elite." *French Politics* 2 (1): 111-123. https://doi.org/10.1057/palgrave.fp.8200054.

Falkowski, Lawrence. 1978. *Presidents, Secretaries of State, and Crises in U.S. Foreign Relations: A Model and Predictive Analysis.* Boulder, CO: Westview Press.

Fawole, W. Alade. 2003. *Nigeria's External Relations and Foreign Policy.* Ile-Ife: Obafemi Awolowo University Press.

Gaddis, J. Lewis. 1992/93. "International Relations Theory and the End of the Cold War." *International Security* 17 (3): 5-58. http://www.jstor.org/stable/2539129?origin=JSTOR-pdf.

Galea, J. 2022. "The Effects of a State Leader's Personality on Foreign Policy Projection: A Case Study of Mintoff's Foreign Policy Towards the Mediterranean." Master Dissertation, Universita ta Malta. https://www.um.edu.mt/library/oar/handle/123456789/106365.

Garba, N. Joseph. 1987. *Diplomatic Soldiering: Nigerian Foreign Policy, 1975-1979*. Ibadan: Spectrum Books.

Gorener, S. Aylin, and Meltem S. Ucal. 2011. "The Personality and Leadership Style of Recep Tayyip Erdogan: Implications for Turkish Foreign Policy." *Turkish Studies* 12 (3): 357-381. https://doi.org/10.1080/14683849.2011.604216.

Greenstein, I. Fred. 1992. "Can Personality and Politics be Studied Systematically." *Political Psychology* 13 (no. 1): 105-128. https://psycnet.apa.org/doi/10.2307/3791427.

Hermann, G. Margaret. 1974. "Leader Personality and Foreign Policy Behavior." In*Comparing Foreign Policies: Theories, Findings, and Methods* edited by James N. Rosenau, 201-234. New York: Sage-Halsted.

___. 1977. "Some Personal Characteristics Related to Foreign Aid Voting of Congressmen." In *A Psychological Examination of Political Leaders* edited by Margaret G. Hermann, 313-334. New York: Free Press.

___. 1980a. "Explaining Foreign Policy Behavior Using the Personal Characteristics of Political Leaders." *International Studies Quarterly* 24 (1): 7-46. https://doi.org/10.2307/2600126.

___. 1980b. "On Foreign Policy Makers, Personality Attributes, and Interviews: A Note on Reliability Problems." *International Studies Quarterly* 24 (1): 67-73. https://doi.org/10.2307/2600128.

___. 2002. "Assessing Leadership Style: A Trait Analysis." Hilliard, Ohio: Social Science Automation, Inc. https://socialscience.net/docs/LTA.pdf.

___. 2005. "Assessing Leadership Style: Trait Analysis." In *The Psychological Assessment of Political Leaders: With Profiles of Saddam Hussein and Bill Clinton* edited by Jerrold, M. Post, 178-212. Ann Arbor, University of Michigan Press.

Hermann, G. Margaret, and Charles F. Hermann. 1989. "Who Makes Foreign Policy Decisions and How: An Empirical Inquiry." *International Studies Quarterly* 33 (4): 361-387. https://doi.org/10.2307/2600518.

Hermann, G. Margaret, Thomas Preston, Baghat Korany, and Timothy M. Shaw. 2001. "Who Leads Matters: The Effects of Powerful Individuals." International Studies Review 3 (2): 83-131. https://doi.org/10.1111/1521-9488.00235.

Hudson, M. Valerie. 2005. "Foreign Policy Analysis: Actor-Specific Theory and the Ground of International Relations." *Foreign Policy Analysis* 1 (1): 1-30. https://doi.org/10.1111/j.1743-8594.2005.00001.x.

Hudson, M. Valerie, and Christopher S. Vore. 1995. "Foreign Policy Analysis: Yesterday, Today and Tomorrow." *Mershon International Studies Review* 39 (2): 209-238. https://doi.org/10.2307/222751.

Houghton, David. 2017. "Political Psychology of Foreign Policy." *Oxford Research Encyclopedia of Politics*. https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-466.

Kaarbo, Juliet. 1997. "Prime Minister Leadership Styles in Foreign Policy Decision-Making: A Framework for Research." *Political Psychology* 18 (3): 553-581. https://doi.org/10.1111/0162-895X.00068.

___. 2021. "New Directions for Leader Personality Research: Breaking Bad in Foreign Policy." *Research Note in International Affairs* 97 (2): 423-441. https://doi.org/10.1093/ia/iiaa221.

Judge, Timothy A., Ronald F. Piccolo, and Tomek Kosalka. 2009. "The Bright and Dark Sides of Leader Traits: A Review and Theoretical Extension of the Leader Trait Paradigm." *The Leadership Quarterly* 20 (6): 855-875. https://doi.org/10.1016/j.leaqua.2009.09.004.

Kesgin, Barış. 2012. "Tansu Ciller's Leadership Traits and Foreign Policy." *Perceptions XVII* (3): 29-50. https://dergipark.org.tr/en/download/article-file/816390.

Kutlu, Erdi, Cagdas Cengiz, Arman M. Necip, and Emir Ozeren. 2021. "Understanding the Role of Leadership Styles of Erdogan and Merkel in Sustainability of Turkey-European Union Relations: A Leadership Trait Analysis." *Sustainability* 13 (16), 9258. https://doi.org/10.3390/su13169258.

Levy, S. Jack. 2013. "Psychology and Foreign Policy Decision-Making" In *The Oxford Handbook of Political Psychology*, 2nd edition, edited by Leonie, Huddy; David O. Sears and Jack S. Levy, 300-333. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199760107.001.0001.

___. 2023. "Foreign Policy Decision-Making: Psychology Dimension." In *The Oxford Handbook of Political Psychology* edited by Leonie, Huddy; David O. Sears; Jack S. Levy and Jennifer Jerit, 3rd edition, 349-391. Oxford: Oxford University Press. https://doi.org/10.1093/oxfordhb/9780197541302.001.0001.

Medeiros, Mike, Alessandro Nai, Aysegul Erman, and Elizabeth Young. 2022. Personality Traits of World Leaders and Differential Policy Responses to the COVID 19 Pandemic." *Social Science & Medicine* 311: 115358. https://doi.org/10.1016/j.socscimed.2022.115358.

Mushtaq, Sadia, and, Ishtiaq A. Choudhry. 2013. "Conceptualization of Foreign Policy: An Analytical Analysis." *Berkeley Journal of Social Science* 3 (spring): 1-21.

Niek, Kok. 2014. "Leadership Trait Analysis: Personality as an Intervening Variable in Foreign Policy." ECPR General Conference Glasgow 03-06 September 2014. https://ecpr.eu/Events/Event/PaperDetails/21610.

Ogwu, U. Joy. 1986. *Nigerian Foreign Policy: Alternative Futures*. Lagos: Nigerian Institute of International Affairs and Macmillan Nigeria Publishers. https://books.google.com.af/books/about/Nigerian_Foreign_Policy.html?id=hc2GAAAAIAAJ&hl=ps.

Ojieh, C. Ojione. 2016. "Extraneous Considerations to the Personality Variables in Foreign Policy Decision-making: Evidence from Nigeria." *Ufahamu: A Journal of African Studies* 39 (2): 197-226. https://doi.org/10.5070/F7392031111.

___. 2008. "Public Opinion and Foreign Policy: Analysing Nigerian Reactions to t h e Asylum Offered Former President Charles Taylor of Liberia." *African Journal of International* Affairs 11 (1): 71-97. https://doi.org/10.4314/ajia.v11i1.57261.

Olusanya, G. Olakunle, and R.A. Akindele. 1986. "The Fundamentals of Nigeria's Foreign Policy and External Economic." In *Nigeria's External Relations: The First Twenty-Five Years*, edited by Olakunle G. Olusanya and R.A. Akindele. Ibadan: University Press Limited.

Pfiffner, P. James. 2004. "George W. Bush: Policy, Politics and Personality." *In New Challenges for the American Presidency* edited by George, C. Edwards III and Davies J., Philip, 161-181. New York: Pearson and Longman. https://pfiffner.schar.gmu.edu/files/pdfs/Book_Chapters/Bush%20Personality,%2004.pdf.

Preston, Thomas. 1997. "Following the Leader: The Impact of U.S. Presidential Style upon Advisory Group Dynamics, Structure, and Decision." In *Beyond Groupthink: Political Group Dynamics and Foreign Policy-making*, edited by Paul 't Hart; Eric, Stern and Bengt Sundelius. Ann Arbor: University of Michigan Press.

Preston, Thomas, and Paul 'T Hart. 1999. "Understanding and Evaluating Bureaucratic Politics: The Nexus Between Political Leaders and Advisory Systems." *Political Psychology* 20 (1): 49-98. https://sci-hub.africa/10.1111/0162-895x.00137.

Puscas, Vasile, and Melania-Gabriela Ciot. 2012. "Psychological Factors in Foreign Policy Decision-Making (I): Decision-Making Models." *Studia Universitatis Babeş-Bolyai. Psychologia-Paedagogia LVII* (no. 1): 53-68. https://doaj.org/article/6c032c50729d4495a6f4275d1d733e10.

Renshon, Jonathan, and Stanley A. Renshon. 2008. "The Theory and Practice of Foreign Policy Decision Making." *Political Psychology* 29 (4): 509-536. https://doi.org/10.1111/j.1467-9221.2008.00647.x.

Pyk, Svitlana. 2024. "Personality Factor Influence in Foreign Policy Decision Making (The Five-Factor Model of Personality Prism)." *Przegląd Strategiczny (Strategic Review)* 17: 217-229. https://doi.org/10.14746/ps.2024.1.15.

Saliu, A. Hassan. 2016. "Is President Buhari De-Marketing Nigeria Abroad?" Paper presented at the30th International Conference of the Nigerian Political Science Association, on the theme "Elections, Security Challenges & African Development, University of Port-Harcourt, Choba, 27th-28th June.

Samson Ezea. 2015. "Controversy Trails Buhari's Policy Announcement Abroad." *The Guardian Newspaper*. https://guardian.ng/politics/controversy-trails-buharis-policy-announcement-abroad/.

Schafer, Mark. 2000. "Issues in Assessing Psychological Characteristics at a Distance: An Introduction to the Symposium." *Political Psychology* 21: 511–527. https://doi.org/10.1111/0162-895X.00201.

Snyder, C. Richard, H.W. Bruck, and Burton Sapin. 1962. *Foreign policy decision making: An Approach to the Study of International Politics*. New York: Free Press.

Suresh, Priya. 2022. "Role of Political Leadership in Foreign Policymaking: Analytical Framework." In: *Foreign Policy of China Under Deng Xiaoping*. Palgrave Macmillan, Singapore, pp. 9-53. https://doi.org/10.1007/978-981-19-4764-3_2.

Thiers, Consuelo. 2025. "Bringing the Leader Back in: The Case for Political Psychology in International Affairs." *RUSI Commentary*. https://www.rusi.org/explore-our-research/publications/commentary/bringing-leader-back-case-political-psychology-international-affairs.

Thiers, Consuelo, and Leslie E. Wehner. 2022. "The Personality Traits of Populist Leaders and their Foreign Policies: Hugo Chavez and Donald Trump." *International Studies Quarterly* 66 (1): 1-11. https://doi.org/10.1093/isq/sqab083.

Winter, G. David. 1992. "Personality and Foreign Policy: A Historical Overview of Research." In *Political Psychology and Foreign Policy*, edited by Eric Singer and Valerie M. Hudson, 79-101. Westview Press. https://doi.org/10.4324/9780429302282.

___. 2003. "Personality and Political Behaviour". In *Oxford Handbook of Political Psychology*, edited by David, O. Sears, Leonie. Huddy and R. Jervis, 110-145. Oxford: Oxford University Press.

Winter, G. David, and A.J. Stewart. 1977. "Content Analysis as a Technique for Assessing Political Leaders." In *A Psychological Examination of Political Leaders*, edited by Margret G. Hermann, 28-61. New York: Free Press.

Young, D. Michael and Mark Schafer. 1998. "Is there Method in our Madness? Ways of Assessing Cognition in International Relations." *Mershon International Studies Review* 42 (no. 1): 63-96. https://repository.lsu.edu/ag_econ_pubs/205.

Zaccaro, J. Stephen. 2007. "Trait-based Perspectives of Leadership." *American Psychologist* 62 (1): 6–16. https://doi.org/10.1037/0003-066X.62.1.6.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Social Networks as Open Sources An Analysis of „Echo Chambers"

Lecturer Raluca LUȚAI, Ph.D.*

*Babeș-Bolyai University, Cluj-Napoca
e-mail: raluca.lutai@ubbcluj.ro

Abstract

This article examines the role of open-source intelligence (OSINT) and, more specifically, social media intelligence (SOCMINT) in understanding emerging social dynamics, focusing on the extremist narratives circulating on the Gab social media platform. As a poorly moderated and ideologically homogeneous environment, Gab functions as an echo chamber in which far-right and white supremacist ideas are generated, amplified, and normalized. Using a passive netnographic methodology, the study analyzes content posted between March and May 2024, identifying patterns of radicalization, hostile narratives, and identity-building processes within two dominant ideological themes: far-right nationalism and white supremacy. The findings demonstrate how social media platforms, whether mainstream or obscure, constitute valuable open sources for identifying early indicators of societal tensions, discursive polarization, and potential offline mobilization. By highlighting how echo chambers shape user perceptions and reinforce extremist worldviews, the article underscores the strategic value of OSINT/SOCMINT for policymakers and security institutions. Ultimately, the study shows that systematic monitoring of online ecosystems is essential for anticipating emerging risks and supporting preventive responses within the broader national security framework.

Keywords:

Open Sources; Social Media Intelligence; Gab; Social Networks.

Article info

Received: 16 November 2025; Revised: 11 December 2025; Accepted: 12 January 2026; Available online: 8 April 2026

Citation: Luțai, R. 2026. "Social Networks as Open Sources. An Analysis of „Echo Chambers."
Bulletin of "Carol I" National Defence University, 15(1): 145-157. https://doi.org/10.53477/2284-9378-26-09

The dynamics of open sources and the emergence of Social Media Intelligence

Open sources represent all publicly available information, collected legally, without requiring privileged access or clandestine means (Hassan and Hijazi 2018, 4). This includes traditional media content, government documents, publicly accessible databases, academic publications, and information generated in the digital environment, particularly on social networks. When data and information from open sources are used to create products that support decision-making, the process is called Open Source Intelligence. Open source data used in the intelligence process can come from radio/TV broadcasts, satellite images, letters of any kind (Hassan and Hijazi 2018, 4). This data represents material that, if taken separately, is not important in the intelligence analysis process, being valuable only when processed alongside other data (Heather and Blum 2018, 10). The first media from which these open sources were collected were books, newspapers, and then radio and TV broadcasts. The importance of open sources was rethought with the emergence and development of social networks, which are now one of the most dynamic and valuable open sources, due to the abundance of information they provide and because they reflect in real time the perceptions, reactions, tensions, and processes shaping public opinion. The emergence of social networks has led to the need to develop a new subdomain of OSINT, as they represent a space where data of interest to analysts is created: Social Media Intelligence. Abbreviated as SOCMINT, it consists of methods, tools, and technology that make it possible to collect and examine data exclusively from social media platforms. It is important to note that Open Source Intelligence (OSINT) is the general framework for collecting, processing, and analyzing information from public sources, while Social Media Intelligence (SOCMINT) is a specialized subdomain of OSINT, dedicated exclusively to data generated in online social media. While OSINT integrates a wide range of sources, from traditional media, official publications, and public databases to satellite imagery, SOCMINT focuses strictly on the dynamics, interactions, and content of user-generated content on social media platforms, providing a type of insight that cannot be obtained by other means.

For information from the internet, including social media datasets, to be used effectively, it must be delivered quickly, securely, and in a way that makes sense to strategic and operational decision-makers. Depending on the objective, the use of SOCMINT can range from simple operational use of a single screen to in-depth strategic analysis (Omand, Bartlett and Miller 2012, 4).
For governments, security agencies, and international organizations, open sources are an essential tool in understanding and monitoring the social environment. Overall, although Social Media Intelligence offers significant advantages such as rapid access to large volumes of data, the ability to monitor events in real time, and an understanding of the structure and dynamics of groups, it also has limitations related to the accuracy of information, the volatility of content, and the difficulty

of filtering relevant data. Beyond these limitations, social networks remain essential because they allow for the early identification of social developments, changes in collective behavior, and emerging discourses that can influence political stability, national security, or social cohesion. Social networks, through the volume and high rate of user-generated content, provide access to a body of information that is difficult to obtain through traditional methods, as they capture both the spontaneous reactions of individuals and the way in which groups build their identity, solidarity, or opposition to certain ideas.

The usefulness of open sources extends significantly to the field of strategic intelligence production[1]. By integrating and analyzing data obtained from these environments, institutions can identify patterns, trends, and emerging phenomena that influence the security environment. Intelligence generated from open sources is not only descriptive but also anticipatory: it allows for the assessment of potential risks, the understanding of radicalization processes, the observation of the dissemination of disinformation and hostile narratives, and the estimation of how certain tensions may translate into concrete actions. This anticipatory capacity is one of the fundamental functions of OSINT/SOCMINT, facilitating the development of preventive policies and strengthening institutional resilience.

[1] Strategic intelligence = a form of analysis that provides a systematic and anticipatory assessment of external developments relevant to the state, used by policymakers to develop national strategies.

In this sense, social networks occupy a central place in the analysis, as they are the space where social dynamics manifest themselves most rapidly and visibly. Mainstream platforms such as Facebook, Twitter/X, or Instagram reflect widespread trends and immediate reactions from the population, while less regulated or obscure networks such as Gab or Telegram provide access to marginal, radical, or emerging discourses that often precede manifestations in the traditional public space. An essential aspect for understanding these platforms is the phenomenon *of echo chambers* (Flaxman, Goel and Rao 2016, 298–320), in which users are predominantly exposed to ideas, opinions, and narratives that confirm their own beliefs. Theoretically, echo chambers work by filtering information and algorithmically structuring digital media so that concordant content is amplified and dissonant content is minimized or excluded. This dynamic favors polarization, the hardening of attitudes, and the consolidation of group identities, as interactions occur in a closed, self-referential environment that constantly reinforces the same perspectives (Del Vicario et al. 2016). In particular, echo chambers are one of the most relevant phenomena for SOCMINT analysis, as they indicate how algorithms and media consumption behaviors influence the aggregation and radicalization of online groups. On obscure platforms, where moderation is low, and users are drawn together by strong ideological affinities, echo chambers become even more pronounced, facilitating the emergence and spread of extreme discourse at an accelerated pace.

Echo chambers formed on various social networks allow governments and institutions to observe both the process of forming dominant opinions and the way in which collective frustrations are aggregated, extremist messages are propagated, and groups with potential influence or risk are mobilized. It is precisely this extended visibility that transforms social networks, whether well-established or lesser-known, into a barometer of the state of society, providing essential clues for anticipating phenomena such as radicalization, polarization, protest mobilization, or the emergence of movements capable of affecting public order (Patel et al. 2020).

Therefore, the importance of open sources, and especially social networks, regardless of their level of notoriety, lies not only in their accessibility but also in their ability to provide a complex, real-time picture of social change. When used appropriately, they become an indispensable strategic resource for understanding developments in contemporary society, for the early identification of emerging risks, and for anticipating collective phenomena with a major impact on national security and stability (Europol 2026). In other words, the systematic integration of open sources into institutional processes becomes not just a methodological option, but a strategic necessity.

Using the tool of netnography, this paper examines how echo chambers are formed on the Gab platform, analyzing two of the most prominent ideological directions present in this environment: the far right and white supremacy. Addressing these issues allows us to understand the processes by which radical discourses are generated, amplified, and normalized in a poorly moderated digital space, where interactions between users are shaped by strong ideological affinities. Studying these phenomena is essential because it provides early clues about the dynamics of radicalization, the consolidation of hostile collective identities, and the potential transfer of violence from the online to the offline space. The analysis of echo chambers and dominant themes on Gab thus contributes to a deeper understanding of emerging risks and is a valuable tool for developing prevention and protection measures in the field of national and social security.

Methodology

Gab.com was chosen as a case study because it is a relatively new social network (launched in 2016), and the context of its emergence, as well as the events subsequently generated through the content distributed, make it a relevant environment for analyzing online extremist phenomena. According to founder Andrew Torba, interviewed by National Public Radio (NPR), the platform was designed as a response to what he called „censorship" practiced by mainstream networks such as Twitter. Torba stated: *I wanted to build an alternative to the big tech oligarchy... I had seen what was happening in Silicon Valley with the rise of censorship during the 2015–2016 election cycle, and I had experienced it myself on Reddit, Twitter, and other platforms. I didn't see any clear and viable alternatives, so I decided to build*

*one myself. Our mission, from day one, has been to defend freedom of expression and individual liberty online for all people (*Public Post 2016).

A decisive factor in selecting this platform for analysis was the 2018 attack on the Tree of Life synagogue in Pittsburgh, which has become a frequently cited case in discussions on the link between online radicalization and offline violence. The perpetrator was highly active on Gab, where he posted and reposted explicitly antisemitic content and threats targeting the Jewish community. Shortly before the attack, he published the message: "I can't sit back and watch my people being sacrificed. Screw public opinion, I'm going in" (public post, 2018), and subsequently killed 11 people (Goodwin 2021).

While this case is often discussed in journalistic investigations, it also reflects broader dynamics identified in the academic literature on online radicalization. Research has shown that poorly moderated or alternative social media platforms can function as echo chambers in which extremist narratives are normalized, reinforced, and increasingly legitimized (Conway 2017; Neumann 2013). Such environments facilitate processes of moral disengagement and grievance amplification, which can contribute to the transition from ideological commitment to violent action (Borum 2011).

Empirical studies further demonstrate a correlation between exposure to online hate speech and real-world violence, suggesting that digital platforms play a significant role in shaping offline behavior (Müller and Schwarz 2020). In this context, Gab has been identified as a space that enables the circulation and mutual reinforcement of extremist discourse due to its minimal content moderation and explicit positioning as a "free speech" alternative (Conway et al. 2019). The Tree of Life attack thus serves as an illustrative case of how online radicalization processes may culminate in offline acts of extremist violence. The data collection period for this study was March–May 2024, a three-month interval chosen to capture a diversity of reactions to local and international events, as well as the dynamics of ideas circulating in the community. The platform was monitored at least once every three days, with a minimum of ten posts selected per session. The content was filtered according to two themes of interest: right-wing extremist nationalism and white supremacy. Blocks of text, images, audio-visual materials, and visible symbols were analyzed, especially those inciting hatred against vulnerable groups such as people of color, Jews, Muslims, or other minorities.

The data collection method followed the principles of netnography, an adapted version of traditional ethnography applied to digital media. Netnography involves direct, systematic, and participatory observation of behaviors, interactions, and discourses in online communities (Bartl, Kannan and Stockinger 2016, 167). Using this method, the researcher can document not only the published content, but also how it is received, reinterpreted, and amplified by community members (Bartl, Kannan and Stockinger 2016, 168).

Ingrid Jeacle points out in „Navigating netnography: A guide for the accounting researcher" (Jeacle 2020, 89). The first category is archival data, which consists of communications and posts made by members of the online community before the researcher joined them and which are accessible to everyone (Jeacle 2020, 89). Passive netnography is the study and observation of this type of data (Costello, McDermott and Wallace 2017, 20). The second category consists of jointly obtained or created data, information that the researcher co-generates with online users during interactions with the group, such as feedback on their own posts, responses to online surveys, and interviews with group members (Jeacle 2020, 90). The researcher participates in a continuous, real-time discourse in this type of active netnography (Costello, McDermott and Wallace 2017, 21). The third category is data produced as a result of field notes taken by researchers while observing the online community (Jeacle 2020, 90). According to this classification, the type of netnography used in this research is passive netnography, focused predominantly on the analysis of archival data. This approach involves non-intrusive observation of content already existing on the platform before the start of the investigation, without direct interaction with community members. We did not actively participate in discussions, we did not intervene in the dynamics of the group, and we did not co-generate data with users, but limited ourselves to periodically monitoring the online space and collecting relevant public posts. Passive netnography is suitable for studying extremist communities because it allows us to capture radicalization processes, dominant discourses, and mechanisms for strengthening group identity without influencing user behavior or altering the nature of interactions between them.

Gab.com. An echo chamber of hate

Gab.com is a social networking site similar to Twitter and Facebook, with over 85.8 million monthly visits (Semrush.com 2026). It was created by Andrew Torba, a businessman and supporter of President Donald Trump who describes himself as a „conservative Christian Republican." What motivated him to start Gab was the desire to create a space for conservatives, who had been unfairly marginalized on Facebook and other social media sites.

According to the information provided in the section „Gab Help Guides - What is Gab.com?", Gab is a social network that promotes „freedom of speech, individual liberty, and the free flow of information online." (Gab.com 2026). Gab quickly became a platform surrounded by controversy (Zannettou et al. 2020, 1008-1009). From the outset, it promoted the idea of almost unlimited freedom of expression, which attracted both supporters of an uncensored internet and much more radical groups. Due to its very permissive content rules, the network became a refuge for far-right individuals and communities, conspiracy theorists, and anti-establishment activists who had been sanctioned or excluded from traditional platforms. Thus, the platform's public image has been shaped at the border between a space of total

freedom and a place where the lack of moderation has allowed the proliferation of controversial and dangerous ideas.

This concentration of radical voices has generated serious criticism. Observers have noted that hate speech, conspiracy theories, and extremist material frequently circulate on Gab without consistent intervention from moderators. Over time, this climate has caused several hosting companies, payment processors, and service providers to distance themselves from the platform, leading to periods where Gab was blocked or forced to rebuild its infrastructure almost from scratch.

The audience using Gab has gradually taken shape. Although it initially attracted people curious to try an alternative to traditional networks, the platform has gradually become a meeting place for those who felt censored or marginalized in the mainstream online space. Many of the users are people interested in intense political discussions, without strict moderation limits.

As the platform's reputation became linked to the idea of „total freedom of expression," Gab attracted diverse groups, from anti-establishment activists and supporters of unconventional political ideas to communities that had been excluded from other networks because of their behavior or discourse. This has resulted in a heterogeneous community, united mainly by the desire to have a space where they can post without fear of sanctions from moderators. Without a doubt, Gab is an expression of an „echo chamber" in which radical opinions amplify each other, and users are exposed almost exclusively to similar ideological perspectives.

In addition to numerous posts promoting hatred and racist content, Gab's lax approach to content has allowed a wave of QAnon conspiracy theories, misinformation, and anti-Semitic comments on the platform. Much of this would not be allowed on today's well-known social networks (e.g., Facebook, Instagram), although they have their own problems in moderating extremism. Promoting „free speech" in an extremist way and broadly defining the concept of freedom of expression, which users invoke whenever they want to justify their malicious actions, creates an environment conducive to the emergence of extremist and hate speech. The toxic environment created within Gab.com should be of interest for studying the role of social networks in Open Source Intelligence analyses.

Nationalism, the far right, and white supremacy

Nationalism and the far right

On Gab, nationalist and far-right ideas are expressed in a visible and often direct manner, shaping the platform's identity over time. In the absence of strict moderation rules, messages glorifying national identity, traditions, and cultural symbols are expressed without restraint. These are often accompanied by anti-globalist rhetoric, which views international institutions and global elites as threats to sovereignty or „authentic" values.

With the mass migration of users excluded from large platforms, Gab has gradually become a refuge for radical voices. In this environment, far-right ideas have become increasingly prominent: xenophobic rhetoric, anti-immigration messages, politically-tinged conspiracy theories, and posts that idealize the past and portray the present as inevitable decline. The symbols, slogans, and themes specific to these movements circulate freely, sometimes even being celebrated by certain internal communities.
The lack of firm moderation has created a space where the line between hardline conservatism and radicalism is blurred. In such a permissive climate, ideas can quickly evolve from simple political opinions to rigid identity discourses, and groups on the fringes of the political spectrum have found fertile ground here to express themselves and attract followers.

The posts identified as falling within the theme of right-wing extremist nationalism discussed any information that would endanger national identity: the users whose posts were collected generally identify themselves as American Christians. Thus, any foreign element (different religion, nationality, ethnicity) represents a threat that, out of loyalty and devotion to their nation, users feel the need to inform the community about and sometimes find solutions to, most often disproportionate ones.

Among the entities frequently targeted by hostile discourse are Ukraine, China, Israel, Muslims, and immigrants. Concerning Ukraine, many users believe that the United States is sending unjustified financial and military aid, ignoring domestic issues such as those in the healthcare system. A common image shows former President Joe Biden alongside Alexandria Ocasio-Cortez, accompanied by the rhetorical question: „Why is there no money for health and social security, but there is money for Ukraine, illegal immigrants, and state-funded colleges?"(public post, April 2024) Ukrainians are sometimes described as a people seeking to profit financially from the US, an idea illustrated by images depicting President Volodymyr Zelensky as the „Queen of Welfare" in a satirical manner. Some posts claim that US support for Ukraine is the result of Jewish influence on US politics, a recurring theme in anti-Semitic narratives on the platform.

Another important direction of these narratives is theories about Israel's influence on US politics. A post shared by @etrimmer features the director of the Bureau of Alcohol, Tobacco, Firearms, and Explosives, Steven M. Dettelbach, accused of wanting to „confiscate Americans' guns," claiming that his intentions are motivated by his Jewish identity. The associated comments reinforce the same conspiracy theme, suggesting that the US is „occupied" or manipulated by organizations such as the Anti-Defamation League. Anti-Semitic discourse occupies a central place in many posts. Jews are blamed for major events such as the 9/11 attacks or caricatured with negative attributes such as „liars," „greedy," „evil," and prone to manipulating the world by playing the victim card in relation to the Holocaust. The narrative that Jews control global institutions or promote social movements such as LGBTQ+

is repeated. In visual representations, the „Happy Merchant" template, considered one of the most widespread anti-Semitic memes, characterized by degrading stereotypes, is frequently used.

Posts glorifying Nazism or far-right figures such as Adolf Hitler or Ursula Haverbeck[2] also appear in these communities. Some messages present Nazism as misunderstood or unfairly „demonized," and Hitler as a sacrificed figure, reinterpreted in a positive light. The posts often receive extensive reactions and explicit support, a sign of the resonance of these ideas in the community. The number of those who support Nazi ideas is numerous. In addition to their admiration for Haverbeck, some users also focus their attention on Adolf Hitler, who is considered a politician who wanted to save the Germans from the Jews and is seen more as a victim than a leader who committed war crimes. @ToddORiley states that „in 1913, Hitler painted Jesus as a child, while the Jews celebrated taking over global finance with the creation of the Fed... History is contaminated..." (public post, April 2024).In addition to such posts, in which Hitler's decisions or quotes are viewed with admiration, there are also those that glorify Nazism in general, by distributing pictures of locations that had the Nazi flag or images of supporters of the extremist ideology.

[2] Ursula Haverbeck (1928–2024) was a German right-wing extremist, best known for denying the Holocaust. Over the years, she was repeatedly convicted of inciting hatred and making public statements contesting and minimizing Nazi crimes.

A constant theme is hostility towards immigrants. Posts such as that of @ Commonsense1774 portray illegal immigrants as armed criminals, while other messages glorify authoritarian policies towards minorities, attributed to leaders such as Vladimir Putin. In the *Trump 2024* group, the discourse describes illegal immigration as an „invasion" permitted or encouraged by the US government, and some users propose radical solutions, such as „a one-way bridge to send Mexicans back."

White supremacy

On Gab, white supremacist discourse is expressed in a direct and unfiltered manner, creating a space where racial identity is transformed into a criterion of human value and social legitimacy. The central discourse that dominates these communities argues that white people are responsible for all the achievements of modern civilization, from political institutions to contemporary technologies, and this perception is accompanied by the idea that other races are inherently inferior or incapable of cultural progress. The posts collected can be grouped into several categories: glorification of the „white man" as the author of civilization, victimization of white supremacists, attribution of negative traits to non-white people, and calls for aggressive action, both online and offline.

In these narratives, white people are presented as rational, disciplined, and moral individuals at the center of human evolution. Examples such as the

post by user @AllAmericanJorge, which justifies the safety of the state of Maine by the fact that the population is „95% white," illustrate the idea that racial homogeneity guarantees peace and public order. In contrast, non-white groups are described as prone to violence or crime, and this perception is constantly reflected in comments and memes distributed within the community. This discourse is supported by messages such as „White people built everything you see" or „White people invented cars, airplanes, and freedom," along with arguments intended to minimize the cultural achievements of people of color or other non-white populations. Images depicting African villages or traditional dwellings are used derisively to create an artificial contrast between „civilization" and „primitivism." At the same time, ideas are propagated about the need to maintain a „white" patriarchy, seen as an indispensable structure for preserving social order and racial supremacy. Profiles such as that of user @Henree, who openly declares his identity as a „national socialist, pro-white," are representative of communities that promote such ideologies.

Victimization is another essential element of white supremacist discourse. Many users claim that they are discriminated against simply because of their identity, that they cannot enjoy their culture or values without being criticized, while minority communities are „encouraged" to express their identity. This leads to claims that „white unity is forbidden" or „just our existence annoys others," creating a false narrative of „white genocide," argued through concepts such as „imposed diversity," considered a strategy to dilute or eliminate the white population. In many of the posts, people of color are portrayed in a degrading manner, being associated with animalistic terms and violent stereotypes. The comments suggest that black people are naturally prone to aggression or criminality, which „excludes" them from the category of „civilized people." This perception is amplified by offensive images, racist jokes, or videos depicting assaults on people of color, distributed not for informational purposes but as a source of entertainment for community members.

In addition to discursive propaganda, there are also calls for direct action. Some users believe that people of color should be „sent back" to the African continent, while others encourage physical aggression or public humiliation. Figures such as @Gypsycrusader are turned into community idols for their videos verbally harassing people of color on video platforms, and their popularity is amplified by the distribution of themed products or racial symbols.

Taken together, the themes of extremist nationalism and white supremacy highlight how the loosely regulated space of the Gab platform fosters the proliferation of radical ideas. While nationalist discourse emphasizes loyalty to the nation and hostility toward certain ethnic or religious groups, white supremacy adds an extra layer of radicalism, articulating a vision in which the white race is presented as the foundation of civilization and as a group in constant danger. Hatred of Jews, Muslims, or people of color is not a new phenomenon on Gab, but the social context and recent events, such as the conflict in Ukraine or internal debates in the United States, have intensified these narratives.

What is worrying is that these discourses do not always remain online. Examples such as the attack on the synagogue in Pittsburgh in 2018 show that digital extremism can turn into real violence, transforming chat rooms into incubators of radicalization. The lack of immediate consequences in the virtual environment and the feeling of impunity fueled by anonymity encourage the expression of increasingly severe forms of hatred, threats, and misinformation.

By analyzing these manifestations, it becomes clear that freedom of expression is distorted in these communities. Any attempt at moderation is perceived as „oppression," and critical reactions are turned into evidence of a conspiracy against the white population. This victimization perspective strengthens internal solidarity but also amplifies the potential for radicalization.

Monitoring platforms such as Gab are essential to understanding the processes through which extremist ideas are formed and propagated. Poorly regulated digital spaces provide fertile ground for the development of movements that can become dangerous in real life. By identifying these dynamics early on, institutions, researchers, and stakeholders can anticipate risks, observe trends in radicalization, and develop appropriate strategies to prevent violence.

Conclusions

This study highlights the growing relevance of open sources in the analysis of social phenomena with implications for national security, demonstrating that digital media, especially social networks, represent a privileged space for early observation of processes of radicalization, polarization, and collective mobilization. The Gab platform, characterized by a low level of moderation and an internal culture that promotes the idea of absolute freedom of expression, functions as a veritable „echo chamber" in which extremist discourse is not only tolerated but amplified and normalized. The analysis of the two themes—right-wing extremist nationalism and white supremacy—shows how online communities can construct hostile identity narratives, reinforce perceptions of victimization, and consolidate polarization mechanisms through repetitive interactions.

By using netnographic methodology and leveraging data from open sources, the paper demonstrates the usefulness of social media analysis in generating strategic intelligence. Observing how such narratives are formed, articulated, and propagated provides institutions with essential insight into emerging risks, enabling early identification of radical developments and tensions that may escalate into violence. Beyond its descriptive dimension, such analysis provides the ability to anticipate, contributing to the formulation of prevention policies and the strengthening of societal resilience. In this sense, research confirms that the systematic monitoring of social platforms, whether mainstream or obscure, is not just an academic exercise but a strategic approach that is indispensable for understanding contemporary realities and protecting national security.

This study is subject to several limitations that should be considered when interpreting the findings. First, the research relies on a passive netnographic approach, focusing exclusively on publicly available, archival content from the Gab platform, without direct interaction with users. As a result, the analysis is limited to observable discursive and symbolic practices and does not capture individual motivations or subjective interpretations of posted content. Second, the data selection is thematically oriented toward far-right nationalism and white supremacy and is not intended to be statistically representative of the entire platform, which may lead to an overemphasis on extremist narratives. The relatively short time frame analyzed (March–May 2024) further constrains the generalizability of the results, as online discourses are highly sensitive to contextual and political developments. Finally, the anonymity of users and the absence of empirical linkage between online discourse and offline behavior limit the ability to assess the real-world impact of the narratives identified, which should be interpreted as indicators of potential risk rather than demonstrated causal relationships.

Building on these findings, future research should expand the temporal and comparative scope of analysis in order to better capture the evolution and persistence of extremist narratives across different platforms and contexts. Integrating longitudinal approaches, cross-platform comparisons, and, where ethically and methodologically appropriate, mixed methods that combine netnography with quantitative or interview-based data could provide a more nuanced understanding of radicalization dynamics and their potential translation into offline action. Such directions would not only strengthen the analytical depth of OSINT/SOCMINT research, but they could also enhance its practical value for anticipating emerging threats and informing more effective prevention and policy responses within the field of national security.

References

Amend Alex. 2018. ”Analyzing a terrorist’s social media manifesto: the Pittsburgh synagogue shooter’s posts on Gab”. https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-Pittsburgh-synagogue-shooters-posts-gab.

Bartl, Michael, Vijai Kumar Kannan, and Hanna Stockinger. 2016. ” A review and analysis of literature on netnography research”. *International Journal of Technology Marketing* 11(2): 165–182. https://doi.org/10.1504/IJTMKT.2016.075687.

Borum, Randy. 2011. ”Radicalization into Violent Extremism I: A Review of Social Science Theories”. *Journal of Strategic Security* 4(4): 7-36. https://www.jstor.org/stable/26463910.

Conway, Maura. 2017**.** ”Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing”. *Studies in Conflict & Terrorism* 40 (1): 77-98. https://doi.org/10.1080/1057610X.2016.1157408.

Costello, Leesa, Marie-Louise McDermott, and Ruth Wallace. 2017. " Netnography: Range of Practices, Misperceptions, and Missed Opportunities". *International Journal of Qualitative Methods* 16(1). https://doi.org/10.1177/1609406917700647.

Del Vicario, Michela, Alessandro Bessi, Fabiana Zollo, Fabio Petroni, Antonio Scala, Guido Caldarelli, H. Eugene Stanley, and Walter Quattrociocchi. 2016. "Echo Chambers in the Age of Misinformation". *Proceedings of the National Academy of Sciences (PNAS)* 113 (3): 554–559. https://doi.org/10.48550/arXiv.1509.00189.

Europol. 2026. " EU Internet Referral Unit - EU IRU, Monitoring terrorism and violent extremism online". https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru.

Flaxman, Seth, Sharad Goel, and Justin M. Rao. 2016. "Filter Bubbles, Echo Chambers, and Online News Consumption". *Public Opinion Quarterly* 80(1): 298–320. doi.org/10.1093/poq/nfw006.

Gab.com. 2026. "Gab.com Help". https://help.gab.com.

Goodwin, Jazmin. 2021. "Gab: Everything you need to know about the fast-growing, controversial social network". https://www.cnn.com/2021/01/17/tech/what-is-gab-explainer/index.html.

Hassan, Nihad A., and Rami Hijazi. 2018. *Open Source Intelligence Methods and Tools*. Berkeley, CA: Apress.

Jeacle, Ingrid. 2020. "Navigating netnography: A guide for the accounting researcher". *Financial Reporting and Accounting* 37(1): 88-101. https://doi.org/10.1111/faam.12237.

Müller, Karsten și Carlo Schwarz. 2021. "Fanning the Flames of Hate: Social Media and Hate Crime". *Journal of the European Economic Association* 19(4): 2131-2167.

Neumann, Peter R. 2013. "The Trouble with Radicalization". *International Affairs* 89(4): 873-893. https://doi.org/10.1111/1468-2346.12049.

Omand, David, Jamie Bartlett, and Carl Miller. 2012. "Introducing Social Media Intelligence (SOCMINT)". *Intelligence and National Security* 27(6): 801–823. http://www.tandfonline.com/doi/abs/10.1080/02684527.2012.716965.

Patel, Faiza, Rachel Levinson-Waldman, Sophia DenUyl, and Raya Koreh. 2020. *Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security.* Brennan Center for Justice at New York University School of Law.

Semrush.com. 2026. "Gab.com – Website Traffic, Ranking, Analytics". https://www.semrush.com/website/gab.com/overview/.

Williams, Heather J., and Ilana Blum. 2018. "Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise". *RAND Corporation*. https://www.rand.org/pubs/research_reports/RR1964.html.

Zannettou, Savvas, Barry Bradlyn, Emiliano De Cristofaro, Haewoon Kwak, Michael Sirivianos, Gianluca Stringhini, and Jeremy Blackburn. 2020. "What is Gab: A Bastion of Free Speech or an Alt-Right Echo Chamber". *WWW ,18: Companion Proceedings of the The Web Conference 2018,* pp. 1007-1014. https://doi.org/10.1145/3184558.3191531.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Armed Conflict in Sudan

Marius-Gabriel BOBOCEA*
*Ministry of Foreign Affairs, Romania
e-mail: marius.bobocea@mae.ro

Abstract

The paper analyzes the armed conflict in Sudan that broke out on April 15, 2023, between the Sudanese Armed Forces (SAF) and the Rapid Support Forces (RSF). Methodologically, the research is based on a qualitative, case study approach, using documentary analysis of UN and UNHCR reports, official communiqués from the governments involved, resolutions and statements from international organizations, as well as the international and regional press. These sources are correlated so as to highlight both the military and geopolitical dimensions, as well as the humanitarian and consular dimensions of the Sudanese crisis.
The results of the research show that Sudan has become an arena for geopolitical competition in which the United Arab Emirates, Egypt, Saudi Arabia, and the Russian Federation project their own interests through military, financial, or diplomatic support to the parties involved in the conflict. A specific result of the analysis is the evaluation of Romania's response as a case study of consular management of a major foreign crisis.

Keywords:
Sudan; Armed Conflict; Abdel Fattah al-Burhan; Mohamed Hamdan Dagalo; RSF; SAF.

Article info
Received: 16 November 2025; Revised: 3 December 2025; Accepted: 13 January 2026; Available online: 8 April 2026

Citation: Bobocea, M.G. 2026. "The Armed Conflict in Sudan."
Bulletin of "Carol I" National Defence University, 15(1): 158-171. https://doi.org/10.53477/2284-9378-26-10

Prolegomena

Sudan is one of the most fragile and conflict-ridden countries on the African continent, its recent history being marked by coups, civil wars, identity fragmentation, and interventions by external actors. Since gaining independence in 1956, the country has endured two major North-South civil wars, the prolonged crisis in Darfur, and, subsequently, the secession of South Sudan in 2011, all of which have eroded internal political cohesion and the capacity of state institutions to manage the competition for power (Collins 2026).

The current conflict has many competing and overlapping dimensions. The violence unleashed by the two rival factions for acquiring control of Khartoum and the surrounding areas has trapped civilians, exposing them to abuse and potential war crimes, food shortages, and the collapse of essential services. The conflict has spread to other regions of the country, with a clear risk of escalation. In addition, Sudan's central importance to regional stability amplifies the stakes for regional and international actors and increases the complexity of finding a negotiated solution to the crisis (Jok, et al. 2023). Studies in *Third World Quarterly* emphasize that *proxy* wars in fragile states tend to be self-perpetuating, as external actors have no real incentives for rapid stabilization.

In this fragile structural context, the current main actors in the conflict emerged and consolidated their positions: the *Sudanese Armed Forces* (SAF) and the *Rapid Support Forces* (RSF). The SAF represents the national army, the traditional pillar of successive regimes in Khartoum, with major political influence in the power structure. Over the decades, the army has been directly involved in coups and the repression of opposition movements, positioning itself not only as the guarantor of territorial integrity but also as a central political actor.
With the support of the regime, the RSF has gradually transformed itself into a powerful paramilitary actor with its own economic resources (including from gold mining) and with a command structure loyal to Mohamed Hamdan Dagalo (*also known as Hemedti*) (Al Jazeera 2023).

Politically, the collapse of O. al-Bashir's regime in 2019[1] created a window of opportunity for a mixed civilian-military government. Civilian leaders, united in coalitions such as the Forces of Freedom and Change, attempted to negotiate a transition to a democratic regime, with Abdalla Hamdok[2] as prime minister. However, competition for control of the state apparatus, disagreements over security sector reform, and, in particular, the integration of the RSF into the SAF

[1] On April 11, 2019, Sudanese President Omar al-Bashir was removed from power by the Sudanese armed forces following widespread protests against his authoritarian regime, thus setting in motion a process of political transition involving both civilian and military leaders.
[2] In 2019, after Bashir's removal, various civilian and military groups, including the *Forces of Freedom and Change* (FFC), negotiated a transitional co-governance agreement intended to lead Sudan toward democratic elections.

have generated major tensions between the army, the RSF, and civilian actors. The military coup of October 25, 2021[3], led by General Abdel Fattah al-Burhan, blocked the transition process, undermined public confidence in the promises of reform, and repositioned the army and the RSF as direct rivals in the competition for power (Al Jazeera 2022).

When religious divisions between communities coexist with other visible structural differences, such as economic inequalities, class affiliation, or linguistic differences, they can become catalysts for separatist movements. These potential flashpoints are often compounded by historical legacies that reinforce perceptions of separation and antagonism (Badal 1976). Analyses in *African Affairs* show that militias partially integrated into state structures eventually become autonomous actors that challenge central authority. This combination of conflictual history, institutional rivalry, and failed political transition shapes the motivation behind the outbreak of armed conflict on April 15, 2023: an open confrontation between the SAF and the RSF for control of the Sudanese state, in an environment where civil institutions are weakened, and regional and international actors exploit Sudan's vulnerability to project their own geopolitical interests.

This paper aims to analyze this conflict, its internal and external dynamics, as well as the humanitarian and diplomatic consequences generated by its prolongation. Thus, the study follows: (1) the genesis and evolution of the RSF from the Janjaweed militias to the status of an autonomous paramilitary actor; (2) the dynamics of the SAF-RSF confrontation and its transformation into a prolonged war; (3) the role of regional and international actors in fueling or managing the conflict; (4) the humanitarian impact and main diplomatic responses, with a focus on Romania's consular protection efforts.

On the humanitarian front, the report highlights Sudan's transformation into one of the most serious humanitarian crises today, with tens of millions of people affected by famine, forced displacement, violence, and limited access to aid. According to Michael Newman[4] the concept of *humanitarianism* can provide a basis for the protection of human beings, not only by conferring legitimacy on the use of military force in truly exceptional situations of human suffering, but also by addressing the problems of poverty and inequality, which are the root causes of the emergencies that humanitarian intervention usually seeks to remedy (Newman 2009). In other words, the intervention of other actors to shorten the conflict is desirable, except that, in this case, Sudan has become an arena for geopolitical competition in which

[3] On October 25, 2021, the Sudanese army, led by General Abdel Fattah al-Burhan, took control of the government in a coup, arresting civilian leaders, including Prime Minister Abdalla Hamdok, which compromised the democratic transition process and strained relations between the military (SAF), paramilitary (RSF), and civilian actors.
[4] British professor and researcher in political science and international relations, known in particular for his contributions to theoretical debates on humanitarian interventions and the responsibility of states in the face of humanitarian crises and mass violence – author of *Humanitarian Intervention: Confronting the Contradictions* în cadrul *Journal of Conflict Studies*.

the United Arab Emirates, Egypt, Saudi Arabia, and the Russian Federation are projecting their own interests through military, financial, or diplomatic support to the parties in conflict. The involvement of these actors does not shorten, but rather contributes to the prolongation and intensification of the war, despite the mediation initiatives of the UN, the African Union, the Arab League, and the Quad format.

A specific result of the analysis is the assessment of Romania's response, through the activation of an inter-institutional task force, the increase in the travel alert level, and the organization of evacuation and repatriation operations for Romanian citizens, as a case study of consular management of a major external crisis. The overall conclusion is that, in the absence of a political agreement between SAF and RSF leaders and coordinated pressure from external actors, the conflict tends to become chronic, with lasting effects on regional stability, security in the Red Sea area, and refugee flows to neighboring states. The selection of sources focuses on official documents from the UN, UNHCR, and the Ministry of Foreign Affairs, as well as reports from international organizations, government statements, relevant international media sources, and academic analyses. This selection allows for a complex triangulation of information between the normative, political, and factual levels.

The contribution of the paper in bringing new elements

The paper highlights several new elements taken from the literature on contemporary armed conflicts and humanitarian crises, especially through an integrated approach to security with the humanitarian and diplomatic fields, treating the conflict in Sudan not only as an internal conflict or a regional proxy war, but, in fact, as a process of isolation and securitization of a humanitarian crisis with direct effects on regional stability (*Horn of Africa, Red Sea*) and on the consular protection policies of third countries. At the same time, the conflict is analyzed as a kind of *multipolar proxy war*, in which competition between regional and extra-regional actors, such as the United Arab Emirates, Egypt, Saudi Arabia, but also Russia and the US, contributes to prolonging this confrontation, making Sudan a point of convergence for competing and current geopolitical interests.

To the same extent, the paper places Sudan within the paradigm of a failed and fragmented state, in which parallel military power factions (SAF vs. RSF) coexist, the absence of a central authority is felt, and there is an institutional inability to regulate and process political transition. In this sense, the correlation between armed violence and the progressive degradation of social order, which highlights the humanitarian crisis manifested in famine, forced displacement, and systematic violence, brings to the fore the instruments of strategic control, and not just the collateral consequences of a conflict.

By introducing the consular-diplomatic dimension as an original case study, through the evaluation of Romania's response to a major external crisis, the paper offers the

reader a rare element in the literature on African conflicts, which largely focuses on the major actors.

In short, the original contribution of the paper is based exclusively on a multi-level analysis, starting at the local level, reaching the regional level, and evoking possible effects at the international level, all of which are a result of the uncontrolled unfolding of the Sudanese conflict. Thus, an exclamation mark is raised in the area of humanitarian crisis and diplomatic implications for third countries.

1. Brief history

Sudan's recent history is marked by armed conflicts between various military groups. The RSF has its origins in the civil war in Chad, the country bordering Sudan to the west. In the 1980s, militias from Chad (supported by Libya) were threatening security in western Sudan (in the Darfur region). As a result, the Sudanese government decided to arm local tribes in Darfur to fight against the militias. The situation worsened in 1983 when the second Sudanese civil war broke out, providing a fertile environment for the militias to operate unchecked. In the following decade, the two groups formed a weak coalition that laid the foundations for the Janjaweed[5] group.

Janjaweed fighters were recruited into the Sudanese state security forces. In 2013, President O. al-Bashir's regime in Sudan faced major and violent protests, which the president suppressed using a Janjaweed faction led by M. H. Dagalo (*Hemedti*). This faction was initially placed under the authority of the Sudanese National Intelligence and Security Service. In 2019, the group supported the Sudanese armed forces in overthrowing President O. al-Bashir, but the two subsequently came into conflict, partly due to plans to integrate the RSF into the SAF.

On October 25, 2021, the Sudanese army, led by General A. F. al-Burhan, took control of the Sudanese government in a military coup. As a result, a state of emergency was declared, many members of civilian Prime Minister Abdalla Hamdock's cabinet were arrested, and the civilian population began to protest, refusing to cooperate with the coup organizers. Subsequently, General al-Burhan, observing internal and international resistance, signed a 14-point agreement whereby Hamdock would become prime minister again. Although Hamdock accepted, he resigned shortly thereafter, on January 2, 2022.

On December 5, 2022, military and paramilitary forces and most civilian leaders signed an agreement to facilitate the transition to civilian rule. However, the population continues to protest, demanding justice for those killed by A.F. al-Burhan's forces.

[5] (Ray 2025) Many believe that this word derives from the Arabic words jinnī (spirit) and jawad (horse).

On January 8, 2023, civilian and military leaders meet to discuss controversial issues, including the integration of the RSF paramilitary forces into the armed forces. Subsequently, in April 2023, based on these discussions, tensions between the SAF and the RSF escalated, erupting into open conflict in the streets of the capital, Khartoum. Civilian leaders, the African Union, and the UN call for an immediate ceasefire, while the parties accuse each other of attacks on their own bases.

2. The armed conflict in Sudan

At present, the African continent is ravaged by armed conflicts, from the Horn of Africa, in the Sahel region, to central Africa. In the Horn of Africa, countries such as Ethiopia (ETH) and Somalia have fallen prey to Al-Shabaab[6] rebels and terrorists from the Islamic State[7], as well as the Tigray[8] group. In the Sahel region, countries such as Mali, Burkina Faso, Niger, and Nigeria are fighting against Al-Qaeda and Boko Haram[9] militias. In the center of the continent, the M23 rebel group[10] has once again become a major threat, especially following its military successes with significant territorial gains in North Kivu province, DR Congo. Also, in the center of the continent, since April 15, 2023, a war has been raging between pro-government armed forces (SAF – led by General Abdel Fattah al-Burhan, leader of the internationally recognized government) and an anti-government paramilitary group (RSF – led by General M.H. Dagalo), plunging Sudan into an unprecedented humanitarian crisis, leaving hundreds of thousands of civilians dead and millions of refugees in its wake.

Initially, fighting took place in the capital Khartoum and in the Darfur district (the western part of Sudan, bordering Chad and the Central African Republic), but it

[6] A militant Sunni group with strong ties to al-Qaeda that controls central and southern Somalia and is engaged in fierce fighting against the Somali government.

[7] The UN officially considers ISIS (also known as ISIL or Daesh) a terrorist group. The UN Security Council has unanimously adopted several resolutions condemning the group's actions and designating it as a threat to international peace and security. Among the most important is Resolution 2199 (adopted in February 2015), which aims, among other things, to block the sources of funding for ISIS and other entities affiliated with Al-Qaeda. ISIS is included on the sanctions list of the UN Sanctions Committee (known as the 1267 Committee), which initially targeted Al-Qaeda and the Taliban and was later expanded to include ISIS.

[8] Officially named the Tigray People's Liberation Front (TPLF), it is a left-wing ethno-nationalist organization that was both a dominant political party and a major paramilitary force in Ethiopia. During the war, the Ethiopian government officially designated the TPLF as a terrorist organization in May 2021. This designation was later revoked in 2023 as part of the peace process.

[9] A radical Islamist terrorist group, active mainly in Nigeria, but also in neighboring countries in the Lake Chad basin region (Chad, Niger, Cameroon). It is considered a terrorist organization by many governments and international organizations. The group also pledged allegiance to the Islamic State (ISIS) in 2015. The Islamic insurgency in Nigeria, led by Boko Haram, has caused a major humanitarian crisis, resulting in thousands of deaths and millions of displaced persons in the West African region.

[10] The M23 group, also known as the *March 23 Movement*, is an armed rebel militia composed mainly of former Congolese army soldiers who have defected. It operates primarily in the eastern Democratic Republic of Congo (DRC). It is an anti-government force fighting against the Congolese armed forces (FARDC). Reports by UN experts and Western governments, including the US and the EU, repeatedly accuse Rwanda and Uganda of providing military and logistical support to the M23, allegations denied by these countries. M23's activities have led to a major conflict, causing a severe humanitarian crisis with hundreds of thousands of people displaced and thousands dead. The group has taken control of key towns in North Kivu province, including Goma. M23 has been accused by human rights organizations of war crimes, including executions, rape, and the forced recruitment of child soldiers.

spread throughout Sudan, culminating in the RSF's capture of the city of El Fasher on October 26, 2025[11]. Thus, at the end of October, the RSF had complete control over the Darfur region and most of the Kordofan region (*the region in central Sudan, to the left of the state capital, Khartoum*). The SAF recaptured much of the capital Khartoum in March 2025 and maintained control over most of the northern, eastern, and central regions, including Port Sudan, where its temporary headquarters are located. (Sudans Post 2025). The actions were condemned by UN Secretary-General Antonio Guterres (United Nations 2025).

Recently, media outlets affiliated with RSF have reported that General Al-Fatih Abdallah Idris[12] was arrested by RSF after a video posted on the Internet showed him killing civilians and soldiers who had surrendered in the city of El Fasher (The Sudan Times 2025). At the same time, the media sources cited mention legal committees investigating the acts committed, with RSF maintaining that they remain committed to respecting human rights and international law.

2.1. Involvement in Sudan's internal affairs by actors in the region, depending on their own geopolitical interests

According to analysts, international relations experts, human rights organizations, and several representatives of Western governments, the United Arab Emirates (UAE), Egypt (EGY), Saudi Arabia (SAU) and the Russian Federation (RUS) are involved in the conflict through various means, including the supply of weapons, financial and logistical support, and diplomatic support to one side or the other (Kottasová 2025).

Human rights experts and activists have noted that the weapons found in Darfur are of Emirati origin, and under the Biden administration, the US (a key ally of the UAE) has highlighted links between a number of companies based in the Gulf nation and the RSF rebels (Kottasová 2025). The accusations are supported by the fact that the UAE wants to destabilize Sudan, ruling out the possibility of democratic elections, an element taken from the UAE's regional campaign against the Arab Spring movements of 2013 (Kottasová 2025). In this context, it is assumed that the Emirati authorities support the commander of the RSF paramilitary organization in Sudan, M.H. Dagalo (*Hemedti*), who allegedly runs a network of companies based in the UAE, in anti-government insurgent actions in Sudan (Kottasová 2025). Despite the fact that a group of experts appointed by the UN Security Council declared (2024) that the allegations were *"credible"*, the UAE vehemently denied the accusations (Kottasová 2025).

[11] On October 26, 2025, the RSF captured the city of El Fasher, the capital of North Darfur district, the last major SAF stronghold in the region. The capture of the city followed a 500-day siege. Media reports focused on violent actions by the RSF, such as atrocities, mass killings, sexual violence, and the destruction of hospitals (G4Media 2025).
[12] Also known by the nickname *Issa Abu Lulu* or, more recently, the *Executioner of El Fasher*. He is a commander within the RSF.

Regarding EGY's interference in Sudanese internal affairs, according to international media (e.g., CNN), Egyptian authorities[13] supported A.F. al-Burhan and M.H. Dagalo in their actions to launch the coup, with the aim of removing the Sudanese president (from 1989 to 2019) F.A. al-Bashir (Kottasová 2025). At the same time, in the current conflict between the RSF and SAF, RSF commander M.H. Dagalo accused EGY of supplying weapons to the Sudanese armed forces and allegedly attacking the RSF, accusations that have been rejected by the Egyptian authorities.

In the context of the SAU's involvement, its support for Sudan is well known, with the evacuation of thousands of civilians since the beginning of the conflict. Although the UAE continues to provide support to pro-government armed forces, implicitly to Commander A.F. al-Burhan, it declares itself neutral in the conflict and is seeking, together with the US, a diplomatic solution to the disagreements between the SAF and the RSF. Peace in the Red Sea is essential for the Saudi economy, given that this region is home to the waterways used for oil exports. Furthermore, the Kingdom's *Vision 2030* project, launched in 2016 by Crown Prince Mohammed bin Salman, is an ambitious national roadmap aimed at transforming the kingdom's economy and society. The main objective of the plan is to reduce the KSA's dependence on oil exports by diversifying the economy and developing new sectors, as well as through major social and cultural reforms.

However, the most significant presence in Sudan is that of the RUS, which sees the conflict in Sudan as an opportunity to deepen its influence in Africa. Previously, according to CNN, the Russian mercenary group Wagner supplied the RSF with missiles through Syria, Libya, and the Central African Republic. The mercenary group has supported militant groups and authoritarian regimes in the Sahel for years in exchange for mineral resources, including major concessions in Sudan's gold mining industry (Kottasová 2025).

Another important element to mention is Moscow's desire to establish its first naval base in the region in Sudan. General Burhan is using this context to negotiate with both the US and RUS. Thus, the international press reports that General Burhan is seeking to establish a US military base, open channels of cooperation in the field of intelligence with Israel through a monitoring center in Port Sudan, and revise Russian, Iranian, and Turkish contracts in exchange for direct political and military support from the US (Kottasová 2025). In this context, this support would be seen as pressure on the UAE to cease military support for the RSF and also to recognize this group as a terrorist organization. In this regard, in his press statement on

[13] Egyptian President Abdel Fattah el-Sisi is a former army general who came to power when he led the 2013 military coup, resulting in the removal of Egypt's first democratically elected president. Since then, A.F. el-Sisi has cracked down on dissent and civil liberties. Several international organizations, including the *United Nations* and *Human Rights Watch*, have expressed serious concerns about the human rights situation in Egypt.

November 11, 2025, Marco Rubio stated that declaring the RSF a terrorist organization is being considered (Rubio 2025).

2.2. The aftermath of the armed conflict in Sudan

According to UN estimates (Ferguson 2025), Sudan is currently experiencing one of the world's worst humanitarian crises, with around 30 million people facing extreme hunger. Furthermore, most of the civilian population has fled their homes, heading for neighboring countries to the west, towards Chad, and to the north, towards Egypt.

According to the UN High Commissioner for Refugees (UNHCR), the latest data from the Egyptian government indicates that since the outbreak of war (mid-April 2023) (UNHCR 2024), over 14 million Sudanese citizens have fled to other locations, leaving their homes, of whom 1.2 million have sought international protection in EGY. In this context, the *Sudan Humanitarian Needs and Response Plan 2024 - HRP*[14] received $1.52 billion in funding, representing 56.3% of the $2.7 billion needed.

Despite this significant contribution, the funding gap remains substantial, underscoring the need for increased international support to meet the growing demands of the crisis (UNHCR 2024). In fact, after nineteen months of conflict in Sudan, thousands of people continue to relocate daily to escape one of the most severe crises in recent decades, which includes famine, brutal violence, abuse, deaths, disrupted services, and limited access to humanitarian aid (UNHCR 2024). Furthermore, on January 7, 2025, US authorities declared that RSF and allied militias had committed acts of genocide (Blinken 2025). *The Journal of Conflict Studies* highlights that securing humanitarian crises shifts the focus from protecting civilians to controlling refugee flows and managing regional risks, but in this case, not only are funds for refugee control insufficient, but attacks on the civilian population continue unabated, raising questions about the possibility of isolating the humanitarian crisis and the risks of regional escalation.

3. Diplomatic efforts

Between May and December 2023, there were numerous attempts at mediation between A. F. al-Burhan (leader of the SAF) and M. H. Dagalo (Hemedti, leader of the RSF), particularly through the initiative of Saudi Arabia and the US, during the negotiations in Jeddah.

Egypt also attempted to organize a direct meeting between the two leaders in the summer of 2024, according to Arab media (*Al-Arabiya, Middle East Eye*), but Burhan refused any meeting with *Hemedti*, considering the RSF a *"rebel" and "illegitimate"* organization (Kiros 2024). At the same time, Egyptian authorities were stepping

[14] Initiated and coordinated by the UN, through its Office for the Coordination of Humanitarian Affairs (OCHA), together with its humanitarian partners. This plan was a collective effort involving numerous UN agencies and non-governmental organizations (NGOs) operating in Sudan, with the aim of providing assistance to people affected by the conflict in the country.

up their contacts within the African Union and the Arab League to confirm the illegitimacy of the RSF. However, later (September 2025), Ambassador Hossam Issa, former Deputy Foreign Minister of EGY and Head of the Department for Sudan and South Sudan, told the Al-Araby Al-Jadeed[15] media trust that the group led by M.H. Dagalo *"will not have a direct impact on EGY, but it is a major problem for Sudan because it entrenches division and leads to the existence of two authorities and the absence of a central government"* (Hornpulse 2025).

According to Al-Araby Al-Jadeed (The New Arab 2025), negotiations were planned (November 25, 2025) between Trump administration representative Massad Boulos and the parties to the conflict, but A.F. al-Burhan refused any meeting with M.H. Dagalo and representatives of the UAE, citing the UAE's bias and support for the RSF rebels, accusing Boulos of promoting a flawed ceasefire plan influenced by the UAE. Al-Burhan considered the US-backed Quad initiative (*US, Saudi Arabia, UAE, Egypt*) to be biased because of the involvement of the Emirates, seeing it as undermining the army while legitimizing the RSF (Booty, Chothia and Chibelushi 2025).

According to the Telegram channel *Middle East Spectator*, which promotes information about the Middle East from the media, contrary to all expectations, on November 6, A.F. al-Burhan and M.H. Dagalo agreed, in principle, to a three-month humanitarian ceasefire under international supervision. On the other hand, on the same date, information appeared (Agenzia Nova 2025) which denied the Sudanese army's agreement to a ceasefire. Thus, according to the decision of the Sudanese Sovereign Council and the statements of A.F. al-Burhan: *"The Council has decided to mobilize the Sudanese people in support of the armed forces to eliminate the rebel militias, as part of the general mobilization and efforts of the state to end this rebellion"* while the SAF *"advances in defeating the enemy and protecting the Sudanese state to its furthest borders"* and *"the attack supported by oppressive and arrogant countries"* (a clear reference to the UAE, an ally of the RSF) would soon be quashed (Agenzia Nova 2025). Subsequently, A.F. al-Burhan promised to avenge the victims of the attacks in North and West Darfur[16], Al Gezira[17] region and other areas, insisting that they are *"on the road to victory very soon"* (Agenzia Nova 2025).

It should be noted, however, that the information appearing on Telegram channels before appearing in official online media outlets was not entirely false. Thus, RSF had accepted the humanitarian ceasefire previously proposed by the US-led mediation group, also known as *The Quad* (*which includes SAU, EGY, and UAE*). This is confirmed in a statement issued by the militias led by General M.H. Dagalo, which

[15] The Al-Araby Al-Jadeed media trust (also known by its English-language version, The New Arab) is a pan-Arab media outlet headquartered in London, UK. Although its headquarters and publishing operations are based in the UK, the trust is owned by the private Qatari company Fadaat Media. It therefore has close ownership and funding ties to Qatar. In addition to its London headquarters, the publication has offices and an extensive network of correspondents in various Arab capitals, including Doha and Beirut.
[16] Administrative regions of the Sudanese state.
[17] Administrative region of the Sudanese state.

stated that a ceasefire *"would ensure the urgent delivery of humanitarian assistance to all Sudanese"* (Agenzia Nova 2025).
In conclusion, the current situation is a belligerent one, with the active involvement of the UN, through mechanisms for providing humanitarian aid to refugees in Sudan, as well as countries such as the US, SAU, EGY and UAE, acting as mediators, each with different interests but, at least officially, the same objective.

4. Consular assistance and protection measures taken by the Romanian Ministry of Foreign Affairs

On April 16, 2023, an inter-institutional *task force* was activated within the Ministry of Foreign Affairs (MAE) to provide assistance to Romanian citizens in Sudan. The task force's efforts were hampered by the fact that the activity of the Romanian Embassy in Khartoum was suspended in 2021, with consular assistance and protection services for Romanian citizens in Sudan being taken over and provided by the Romanian Embassy in Addis Ababa, ETH.
The MFA, through a larger number of Romanian diplomatic missions and in collaboration with institutional partners, took numerous steps to identify and contact Romanian citizens and their family members in Sudan, as well as to establish optimal evacuation methods.

On April 17, 2023, the travel alert level was raised to 8 out of 9 - *Avoid all travel.* (Ministry of Foreign Affairs 2025) and recommended that all Romanian citizens still in Sudan make their presence known by contacting the Romanian diplomatic mission in Ethiopia and requesting consular assistance if they wish to be evacuated (Ministry of Foreign Affairs 2023). Thus, from the convening of the interinstitutional task force by Foreign Minister Bogdan Aurescu (April 16, 2023) until May 3, 2023 (Ministry of Foreign Affairs 2023), 46 people (39 Romanian citizens and 7 of their family members, who are foreign nationals) were evacuated from Sudan. Evacuation operations from the conflict zone and repatriation to Romania were carried out and completed together with European partners. Thus, with a view to coordination at EU Member State level, representatives of the Consular Department participated in the extraordinary informal meetings of the Consular Affairs Working Group (COCON) of the CONS organized by the Swedish Presidency in videoconference format and accessed the CoOL (Consular online) platform, which proved to be a useful tool for the real-time exchange of information on various aspects of crisis management. Thus, with the support of the French, Swedish, Greek, and British authorities, air evacuations were carried out to various countries, such as Djibouti, Cyprus, and Greece. Support and assistance were also provided to Romanian citizens and their family members who traveled by road to EGY and ETH or by sea to SAU. The Ministry of Foreign Affairs headquarters and the Romanian diplomatic missions involved provided the necessary support for subsequent repatriation to Romania, including domestic transport and transport to the final destination, the issuance of travel documents to the Romanian citizens in question who no longer had valid documents, and the completion of all transit formalities.

Regarding the position of the Romanian Ministry of Foreign Affairs on the armed conflict in Sudan, its representatives hope for a peaceful and sustainable resolution of the situation in Sudan, as confirmed during the reception by Secretary of State Traian Hristea of the Ambassador of the Republic of Sudan to Romania, Almansour Ibrahim Bolad, on the occasion of his farewell visit (Ministry of Foreign Affairs 2024). Romania's position is linked to the fact that resolving the conflict, restoring the rule of law, and taking the necessary steps for the reconstruction of Sudan will allow for the consolidation and deepening of Romanian-Sudanese cooperation, including in the field of democratic transition.

Conclusions

Since April 15, 2023, Sudan has been embroiled in an armed conflict between the Sudanese Armed Forces (SAF) and an anti-government paramilitary faction (RSF) fighting for power. African states are familiar with such conflicts, most of them facing them frequently.

Even though this conflict was predicted by the international media, analysts, and officials of other states to be short-lived, the two warring forces have taken actions that have prolonged the conflict to more than three years. As a result, Sudan is becoming increasingly vulnerable and weakened in the face of armed conflict, with its population turned into refugees and displaced persons, without any viable medium- or long-term solutions.

The population of Sudan, estimated at around 50 million in 2024, is currently facing severe famine. At the same time, since the beginning of the conflict, more than 150,000 civilians have been killed, mainly during the capture of El Fasher by the RSF, and more than 12 million people have been displaced by the fighting. Furthermore, violence, mass killings, and abuse of women are part of the RSF's strategy to dominate parts of Sudan. In the absence of diplomatic strategies initiated by mediating states to bring the two commanders (M.H. Dagalo and A.F. al-Burhan) to the negotiating table, the humanitarian crisis in Sudan will deepen to such an extent that neighboring states will feel the pressure of refugees, and the UN will have to find measures to rebuild a state and uprooted generations.

Implications for public policy

In terms of public policy, the paper conveys the need to correlate security and humanitarian policies in order to avoid treating refugees exclusively as a risk. Thus, it highlights the importance of strengthening consular response and coordinated evacuation mechanisms at the EU level, based on lessons learned from the Sudan case. Integrating humanitarian access into regional security strategies by increasing coordinated diplomatic pressure on external actors fueling the conflict, including through targeted sanctions, may be one of the most profoundly beneficial outcomes for the affected population in any type of conflict.

Limitations

The main limitations in writing this material were both the lack of access to data and information from the field, which could have been disseminated through interviews or transcribed through direct observation, and the fluid nature of the conflict, which could lead to the perishability of some assessments. It should also be noted that it was difficult to independently verify information from areas controlled by the RSF or SAF, and that it was only possible to consult certain biased media sources, potentially affiliated with regional actors involved in the conflict.

Proposals and future directions for research

In order to increase the visibility of strategies for resolving or, at least, managing societal crises arising from conflicts, numerous comparative analyses of the management of such crises at the consular level are needed. Thus, a study of the impact of proxy wars on displaced children and generations as a factor of long-term insecurity could be prepared and debated, from which lessons could then be drawn as a basis for further studies. Such a study could take into account factors such as the role of transnational companies and economic networks in financing armed conflicts, and the evaluation of the effectiveness of multilateral mediation formats in conflicts with autonomous paramilitary actors.

References

Agenzia Nova. 2025. "Armata sudaneză respinge propunerea de armistițiu: „Vom lupta până când RSF va fi învinsă"." *Agenzia Nova.* https://www.agenzianova.com/ro/news/Armata-Sudanului-respinge-propunerea-de-armisti%C8%9Biu%3B-vom-lupta-p%C3%A2n%C4%83-c%C3%A2nd-RSF-va-fi-%C3%AEnfr%C3%A2nt%C4%83./.

Al Jazeera. 2023. "Sudan-unrest-what-is-the-rapid-support-forces." *Al Jazeera*. https://www.aljazeera.com/news/2023/4/16/sudan-unrest-what-is-the-rapid-support-forces.

___. 2022. "Timeline: Sudan's political situation since al-Bashir's removal." *Al Jazeera*. https://www.aljazeera.com/news/2021/10/25/timeline-sudan-since-the-fall-of-omar-al-bashir.

Badal, R.K. 1976. "The rise and fall of separatism in Southern Sudan." A*frican Affairs* 75 (301): 463–474. https://doi.org/10.1093/oxfordjournals.afraf.a096771.

Blinken, Antony J. 2025. "Genocide Determination in Sudan and Imposing Accountability Measures." *US Department of State*. https://2021-2025.state.gov/genocide-determination-in-sudan-and-imposing-accountability-measures/.

Booty, Natasha, Farouk Chothia, and Wedaeli Chibelushi. 2025. "A simple guide to what is happening in Sudan." *BBC*. https://www.bbc.com/news/articles/cjel2nn22z9o.

Collins, Robert O. 2026. "Sudan". *Britannica*. https://www.britannica.com/place/Sudan.

Ferguson, Sarah. 2025. "Famine Takes Hold in Sudan". *UNICEF*. https://www.unicefusa.org/stories/famine-takes-hold-sudan?utm_source=bing&utm_medium=cpc&utm_campaign=202511_eme_Sudan_en_M_Search&utm_content=2025_Sudan_Famine_M_Search&initialms=bing__cpc__202511_eme-rv_other-sem__textonly_na_na_na_na_sudan&msclkid=0b36.

Hornpulse. 2025. "Cairo-moves-to-counter-hemedtis-parallel-government-in-sudan." https://hornpulse.com/2025/09/01/cairo-moves-to-counter-hemedtis-parallel-government-in-sudan/.

Jok, Jok Madut, Anette Hoffman, Dan Watson, and Benjamin Petrini. 2023. "Conflict Briefing on Sudan: Roots of the war, regional implications, and the way forward." *Third World Quarterly*. https://www.iiss.org/events/2023/05/conflict-briefing-on-sudan-roots-of-the-war-regional-implications-and-the-way-forward/.

Kiros, Kidane. 2024. "The Ongoing War in Sudan and Its Implications for The Security and Stability of The Horn of Africa and Beyond." Policy Center for the New South. https://www.policycenter.ma/publications/ongoing-war-sudan-and-its-implications-security-and-stability-horn-africa-and-beyond.

Kottasová, Ivana. 2025. "Sudan's bloody conflict is plagued by foreign influence – here is what we know." *CNN*. https://edition.cnn.com/2025/11/07/africa/sudan-conflict-foreign-influence-intl-cmd.

Ministry of Foreign Affairs (MAE). 2023. "Precizări de presă privind demersurile MAE în contextul evoluției situației de securitate din Sudan." https://www.mae.ro/node/61711.

___. 2024. "Primirea de către secretarul de stat Traian Hristea a ambasadorului Republicii Sudan în România, Almansour Ibrahim Bolad cu prilejul vizitei de rămas bun." https://www.mae.ro/node/64597.

___. 2025. "Sudan." https://www.mae.ro/travel-alerts/2924.

Newman, M. 2009. "Humanitarian Intervention: Confronting the Contradictions." *Journal of Conflict Studies*. https://journals.lib.unb.ca/index.php/JCS/article/view/15249/24249.

Ray, Michael. 2025. "Janjaweed." *Britannica*. https://www.britannica.com/topic/Janjaweed.

Rubio, Marco. 2025. "Secretary of State Marco Rubio Remarks to the Press." *US Department of State*. https://www.state.gov/releases/office-of-the-spokesperson/2025/11/secretary-of-state-marco-remarks-to-the-press.

Sudans Post. 2025. "Territorial-control-in-sudan-october-2025." *Sudans Post*. https://www.sudanspost.com/territorial-control-in-sudan-october-2025/.

The New Arab. 2025. "US envoy urges Sudan warring sides to accept ceasefire proposal." *The New Arab*. https://www.newarab.com/news/us-envoy-urges-sudan-warring-sides-accept-ceasefire-proposal.

The Sudan Times. 2025. "Who-is-issa-abu-lulu-the-butcher-of-el-fasher." *The Sudan Times*. https://thesudantimes.com/sudan/who-is-issa-abu-lulu-the-butcher-of-el-fasher/.

UNHCR. 2024. "Egypt-now-biggest-recipient-sudanese-forced-flee-ongoing-war." *UNHCR*. https://www.unhcr.org/eg/news/egypt-now-biggest-recipient-sudanese-forced-flee-ongoing-war.

United Nations. 2025. "Secretary-General Expresses Grave Concern over Military Escalation in El Fasher, Sudan, Urges Parties to Engage with Personal Envoy." *United Nations*. https://press.un.org/en/2025/sgsm22883.doc.htm.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Military-Industrial Complex in the Transnistrian Region: a Threat to the National Security of the Republic of Moldova

Professor Svetlana CEBOTARI, Ph.D. habilitate*
Div. General (r) Ion COROPCEAN, Ph.D.**

*Department of International Relations, Faculty of International Relations, Political and Administrative Sciences, State University of Moldova; "Alexandru cel Bun" Military Academy, Chisinau, Republic of Moldova
e-mail: svetlana.cebotari11@gmail.com
https://orcid.org/0000-0001-9073-104X

**Agency for Science and Military Memory, State University of Moldova, Chisinau, Republic of Moldova
e-mail: ion.coropcean@gmail.com
https://orcid.org/0000-0001-8793-4065

Abstract

The military-industrial complex in the Transnistrian region of the Republic of Moldova, a territory outside the effective constitutional control of state authorities, constitutes a major risk factor to national security. This article analyzes the military, political, and geopolitical dimensions of this complex, highlighting its destabilizing impact on the security architecture of the Republic of Moldova and the South-Eastern European region. The article also examines the historic evolution and current activities of several industrial enterprises in the Transnistrian region involved in the unauthorized production and storage of weapons and ammunition, as well as the strategic relevance of the Cobasna military depot, considered one of the largest storage facilities for conventional ammunition in South-Eastern Europe. Thus, the research demonstrates that maintaining the military-industrial complex and significant ammunition stockpiles in the Transnistrian region generates persistent threats to the security of the Republic of Moldova, while also contributing to regional instability and increased risks to European security.

Keywords:
Transnistria; Military-Industrial Complex; National Security; Cobasna Depot; Ammunition; Russian Federation; Republic of Moldova.

Article info
Received: 22 January 2026; Revised: 2 February 2026; Accepted: 2 March 2026; Available online: 8 April 2026

Citation: Cebotari, S., and I. Coropcean. 2026. "The Military-Industrial Complex in the Transnistrian Region: a Threat to the National Security of the Republic of Moldova." *Bulletin of "Carol I" National Defence University*, 15(1): 172-193. https://doi.org/10.53477/2284-9378-26-11

The national security environment of the Republic of Moldova is significantly shaped by the unresolved conflict in the Transnistrian region, which continues to generate structural vulnerabilities across political, military, economic, and societal levels. In this context, the military-industrial complex developed on the territory of the Transnistrian region represents a major risk factor that remains insufficiently analyzed in the specialized literature, yet has direct implications for the stability of the Republic of Moldova and for regional security. The persistence of industrial capacities with a military profile, inherited from the Soviet period and adapted to new geopolitical realities, contributes to the maintenance of a power imbalance and to the perpetuation of a climate of insecurity in the immediate vicinity of the Republic of Moldova's borders.

The military-industrial complex in the Transnistrian region is characterized by a high degree of institutional opacity, the absence of control by the constitutional authorities of the Republic of Moldova, and ambiguous connections with external state and non-state actors. It encompasses production, repair, and storage infrastructures for military equipment, as well as underground economic networks that may facilitate the illicit trafficking of weapons and dual-use technologies. In the absence of a functional legal and political framework for international monitoring, these industrial capacities may be instrumentalized both for military purposes and as levers of geopolitical pressure, thereby amplifying hybrid risks to the security of the Republic of Moldova.

Analyzing the Transnistrian military-industrial complex as a threat to national security requires an interdisciplinary approach that integrates perspectives from security studies, international relations, political economy, and international law. This research aims to highlight the role and functionality of this complex within the regional security architecture, to identify the mechanisms through which it undermines the sovereignty and defense capacity of the Republic of Moldova, and to contribute to the formulation of scientifically grounded public policies and security strategies. In a geopolitical context marked by instability and intensified strategic competition in Eastern Europe, the investigation of this topic becomes not only relevant but imperative for understanding current and future challenges to Moldovan statehood.

To conduct the present research on the military-industrial complex in the Transnistrian region as a potential threat to the security of the Republic of Moldova and to highlight the main repercussions it may generate for national security, a coherent set of general and specific research methods was employed. The adopted methodological approach seeks to explain the manner and extent to which the Transnistrian military-industrial complex constitutes a risk factor, moving beyond strictly descriptive approaches and orienting the analysis toward causal relationships, functional mechanisms, and systemic effects.

The examination of the military-industrial complex from both conceptual and operational perspectives was made possible by analytical and deductive methods, which facilitated the identification of the main dimensions of the threat to the Republic of Moldova's security. The analysis is grounded in an interdisciplinary theoretical framework situated at the intersection of security studies, critical political economy, and international relations, enabling the clarification of the conceptual benchmarks associated with the notion of the military-industrial complex. This interpretative framework allows for an understanding of the Transnistrian phenomenon not merely as a set of arms production or storage capacities, but as an informal politico-economic network integrated into a regional system of influence and control.

Documentary analysis constitutes the primary data collection method and focuses on relevant academic studies, open-source intelligence (OSINT), reports from international organizations, and investigative media materials. Complementarily, qualitative content analysis is applied to identify strategic narratives and security discourses associated with the Transnistrian military-industrial complex, thereby extracting latent meanings from official and unofficial sources and highlighting how this phenomenon is legitimized, minimized, or instrumentalized in political and media contexts. Furthermore, the research integrates *diachronic comparative analysis*, tracing the evolution of the region's military-industrial infrastructure in relation to post-Soviet geopolitical transformations and the dynamics of the frozen conflict in the Republic of Moldova. By correlating historical data with recent information, it was possible to formulate plausible inferences regarding the current function of this complex and its impact on regional security.

The case study is an essential component of the research, facilitating an in-depth analysis of the military-industrial complex's repercussions in the Transnistrian region on the security of the Republic of Moldova. This method enabled examination of interactions among military, economic, and political factors within an externally supported separatist space, including relevant sub-cases such as inherited Soviet-era military infrastructure and enterprises with military or dual-use profiles. To assess the impact on national security, *risk analysis* was employed, structured around three main dimensions: the probability of threat manifestation, its destructive or destabilizing potential, and the degree of control exercised by the constitutional authorities of the Republic of Moldova. This methodological approach allows for a transition from descriptive observations to the formulation of conclusions with strategic relevance.

Given the fact that, within the academic literature of the Republic of Moldova, there are no comprehensive studies dedicated to the analysis of the military-industrial complex in the Transnistrian region as a threat to state security, the *webographic method* was also applied. This method enabled examination of the subject at both theoretical and practical levels by using relevant online sources, contributing to a broader, more up-to-date understanding of the issue under investigation.

At the same time, the use of the *phenomenological method* enabled the analysis of the essential dimensions of the studied phenomenon, thereby facilitating the investigation of experiences, perceptions, and structures of meaning associated with the Transnistrian military-industrial complex. In the context of the war in Ukraine, triggered by the invasion of the Russian Federation, regional security concerns have regained heightened importance, bringing to the forefront the need to reassess the role of the military-industrial complex in the Transnistrian region. In this regard, the historical method made it possible to analyze the specific conditions of setting and the evolution of this complex, offering a diachronic perspective on its transformations and their implications for the security of the Republic of Moldova. Considering that the Russian Federation conceals certain data or provides misleading information regarding the military-industrial complex in the Transnistrian area, the methodology employed in the elaboration of this article was predominantly qualitative and inductive in nature, combining critical analysis of open sources with informational triangulation and comparative evaluation of official and alternative narratives. The adopted methodology provides a coherent framework for analyzing the military-industrial complex in the Transnistrian region of the Republic of Moldova and contributes to the development of security research in the Eastern European context. By integrating multiple qualitative methods, the study ensures a comprehensive and rigorous approach to the phenomenon under analysis.

„The military-industrial complex" — a conceptual and theoretical approach

For a better understanding of the issue concerning the military-industrial complex in the Transnistrian region of the Republic of Moldova, it is necessary to clarify the meaning of the concept of the military-industrial complex (MIC). The term "military-industrial complex" was famously used by U.S. President Dwight D. Eisenhower in his farewell address on January 17, 1961 (Britannica 2025). Eisenhower warned that the United States must "guard against the acquisition of unwarranted influence … by the military-industrial complex" (National Archives 1961). According to Eisenhower's perspective, the military-industrial complex tends to promote policies that may not align with the national interest (such as participation in a nuclear arms race), and he believed that its growing influence, if left unchecked, could undermine American democracy (Reaching Critical Will 2025).

Although this expression is commonly attributed to Eisenhower (Oxford 2001, 82), and many scholars initially regarded the phenomenon as novel, characteristics associated with the domestic and international military-industrial complex can be identified prior to his landmark speech. The term "military-industrial complex" was first employed by C. Wright Mills in 1956 (Mintz 1985), and elements of such a complex can be traced throughout the history of warfare, dating back to the earliest stages of civilization. As Keith Nelson notes in his work on the constitutive traditions of the military-industrial complex, "those traditions that hold rulers, soldiers,

and merchants responsible for war have pursued their separate paths over many centuries." Nevertheless, the first concrete roots of the modern military-industrial complex can be identified in the United States at the turn of the late nineteenth and early twentieth centuries (Salisbury 2024, 14–21).

The term "military-industrial complex" may also refer to the physical concentration of military production. Military expenditures generate spatial clusters of prime contractors, subcontractors, consultants, universities, skilled labor, and government facilities, all dedicated to research and development or the manufacture of military systems and technologies. Notable examples include the aerospace complex of Southern California, the shipbuilding complex along the southern coast of South Korea, and the isolated military research center of Akademgorodok in Siberia. National governments have often created such complexes in areas lacking a prior industrial tradition by guaranteeing large-scale migration of skilled labor. These areas came to resemble company towns, providing not only employment but also housing, healthcare, and education for workers and their families. During the Cold War, the military-industrial complex constituted a major center of power, and today its influence is even greater, serving as a critical link between the armed forces and the industries that manufacture military equipment. Koistinen argues that the MIC represents a recognized process through which multiple institutions—most notably the military and commercial enterprises—collaborate to provide the state with the operational capabilities required for warfare (Koistinen 1980, 1).

In the work *"Delta of Power",* Alex Roland presents a comprehensive history of the CMI from 1961, the Cold War, and the War on Terrorism, to the present. Roland contends that the MIC is now significantly different from the form it assumed when Eisenhower warned of its dangers, continuing to exert considerable, though diminished, influence over American life. Focusing on the three decades following the end of the Cold War in 1991, Roland explains how fragmentation, rapid change, and historical contingency transformed America's military-industrial institutions and infrastructure. He identifies five critical areas of transformation: civil–military relations; relations between industry and the state; inter-agency relations within government; relations between scientific-technological communities and the state; and the relationship between technology and society (Roland 2001).

At the core of any definition of the military-industrial complex lies the existence of a strong defense industrial base around which state interests may coalesce. The MIC becomes a self-generating structure (agency) that embodies the interests of various societal groups. The strength of entrenched interests and their competition for resources generates internal pressure for increased military spending, while external threats are often exaggerated to provide the necessary justification (Dunne and Sköns 2009).
Since Eisenhower's speech, the expression "military-industrial complex" has acquired multiple meanings. The Vietnam War context added its own nuances to

definitions developed during and after that period, and the end of the Cold War and the beginning of the "Global War on Terrorism" led to new changes in meaning. Nevertheless, the term is almost always employed pejoratively and serves as a useful analytical tool for many authors addressing broader structural tendencies. There are no entirely impartial analyses of the military-industrial complex; each approach contains a critique or series of critiques, through which the evolution of the concept over time must be discerned. As James Ledbetter observes, the military-industrial complex is "a rhetorical Rorschach blot — the meaning depends on the eye of the beholder" (Salisbury 2024, 14). The picture is also complicated by the fact that the suffix "industrial complex" has become a rather worn-out way of suggesting that policy in any field has been undermined by profit motives: in criminal justice, healthcare, and many others.

Other definitions of the military-industrial complex suggest that it encompasses the armed forces and all businesses and government agencies that support them. Weapons manufacturers and politicians who accept donations from such companies are considered part of the military-industrial complex. A company that produces weapons contributes to a politician's campaign; following elections, that legislator increases military funding, which is then used to purchase tanks, weapons, and ammunition from the same company (Vocabulary 2025). The military-industrial complex, initially considered an exclusively American phenomenon of the Cold War, was adapted to develop and produce military technologies at the level of the existential threat perceived as being represented by the Soviet Union. An informal yet robust relationship between the military and industry, the military-industrial complex pursued and won a race for technological development.

Thus, based on these interpretations, the military-industrial complex may be understood as the relationship among a country's military, its government, and the defense industry that supplies weapons and services. This concept highlights the way how these entities interact and mutually reinforce one another, shaping national policies and economic priorities, particularly during periods of intensified military engagement. The military-industrial complex became a significant factor in shaping both U.S. foreign and domestic policy during the Cold War and continues to play a role in contemporary governance (Fiveable 2025).

The military-industrial complex in the Transnistrian region

The security challenges of the Republic of Moldova cannot be rigorously examined without integrating the Transnistrian dimension, a territory that has remained outside the effective control of the constitutional authorities for more than three decades. The territory of the administrative unit on the left bank of the Dniester River covers approximately 4,000 km², representing approximately 12 percent of the Republic of Moldova's total area. From a factual perspective, the self-proclaimed entity known as the "Pridnestrovian Moldavian Republic" does not fully overlap

with the Transnistrian region, as six communes situated east of the Dniester River - Cocieri, Molovata Nouă, Corjova, Coșnița, Pârâta, and Doroțcaia - remain under the jurisdiction of the constitutional authorities of the Republic of Moldova. At the same time, the de facto administration in Tiraspol exercises control over the municipality of Bender (including the locality of Proteagailovca) and over the communes of Gâsca and Chițcani, located west of the Dniester River. In parallel, the Dubăsari district is administratively divided into two distinct entities: one under the authority of the constitutional government in Chișinău and the other under the separatist administration in Tiraspol (Țăranu 2024, 182).

This fragmented territorial-administrative configuration has not only political and legal implications but is also closely linked to the legacy and persistence of the military-industrial complex in the region. During the Soviet period, the Transnistrian space was designed as a strategic node of the defense industry, concentrating military production units, logistical infrastructure, and weapons storage facilities deliberately positioned near major transportation axes and along the western frontier of the Soviet Union. Following the dissolution of the USSR, these capacities were not fully dismantled; instead, they became one of the material pillars of the consolidation of the separatist regime, providing both economic resources and instruments of coercion. Enterprises associated with the military-industrial complex are located on the left bank of the Dniester, primarily in the cities of Tiraspol and Rîbnița (see *Figure* 1). The control exercised by the de facto authorities in Tiraspol over key localities on the right bank of the Dniester, such as the municipality of Bender, must also be interpreted through the lens of their strategic importance within the architecture of the former military-industrial complex, as these areas ensure access to critical infrastructure, communication routes, and industrial facilities with dual-use (civil–military) potential.

In this context, although the armed conflict on the Dniester formally ended in 1992, its structural effects cannot be dissociated from the security and industrial logic inherited from the Soviet period, which continues to shape local power relations and to significantly condition the prospects of state reintegration. One of the most sensitive and persistent elements of this legacy is the existence of a military-industrial complex derived from the strategic infrastructure of the former Soviet Union. This complex is not merely a historical relic but a functional reality with considerable destabilizing potential. The presence of the ammunition depots at Cobasna, industrial capacities dedicated to the production and repair of armaments, and the associated parallel economic networks transform the Transnistrian region into a vector of insecurity not only for the Republic of Moldova but also for the broader space of Southeast Europe. Over time, these resources have been instrumentalized both politically and economically, serving as mechanisms of strategic pressure, destabilizing factors, and potential sources of latent conflict with regional implications.

TIRASPOL
Industrial enterprises:
„Pribor", „Metalorucav",
„Kirov Electrical
Appliances".
The industrial complex
„Electromaș."

RÎBNIȚA
Metallurgical and hydraulic
industrial complex

Figura 1 The main locations of the military-industrial complex of the Transnistrian region
Source: based on research developed by the authors

The specialized literature and reports of international organizations converge in assessing the Transnistrian military infrastructure as a major security risk. Thus, Peterka-Benton (2012) emphasizes the region's traditional role as a hub within illicit small-arms trafficking networks, while analysis by the Global Initiative (2024) points to a reactivation of illicit arms flows following the outbreak of the war in Ukraine. This development once again places the Transnistrian region at the center of the regional security equation.

Within the same analytical framework, the Organization for Security and Co-operation in Europe (OSCE 2024) has repeatedly highlighted existing structural vulnerabilities and the need to strengthen the Republic of Moldova's institutional capacities to manage risks related to the proliferation of small arms and light weapons. Complementarily, internationally renowned media outlets, such as the Financial Times (Financial Times 2025), have underscored the geopolitical dimension of the issue, revealing how the military infrastructure of the Transnistrian region is used as an instrument of external pressure within the context of regional strategic competition.

Viewed from this perspective, the Transnistrian region transcends the status of a purely local problem and emerges as a constitutive element of a broader geopolitical puzzle, in which organized crime, illicit arms trafficking, and external political interests intersect and mutually reinforce one another. The threat generated by the

Transnistrian military-industrial complex can be conceptualized through several interconnected mechanisms:

Illegal production and repair of weapons. Industrial capacities inherited from the Soviet period, although significantly reduced compared to their original scale, continue to enable limited-scale production, modernization, and refurbishment of small arms. This reality keeps the region in a state of constant risk, facilitating its integration into illicit arms circuits and supplying regional black markets.

Ammunition depots. The Cobasna ammunition storage complex, which houses tens of thousands of tons of conventional ammunition, represents a permanent source of insecurity. The associated risks are manifold, ranging from the potential diversion of stockpiles into illicit trafficking networks to environmental and technogenic threats generated by the degradation of expired munitions and the possibility of major incidents with cross-border impact.

Smuggling networks and the parallel economy. The Transnistrian region is characterized by informal economic flows and a "grey" economy that also facilitates arms trafficking. These networks contribute to the consolidation of political and financial dependencies, perpetuate corrupt practices, and undermine the Republic of Moldova's capacity to exercise effective control over its own security space.

Politicization of military infrastructure. The Transnistrian military-industrial complex is not merely a technical or security-related issue but is deeply embedded within a political and geopolitical logic. Its existence and preservation serve as instruments of hybrid pressure, employed by both the de facto regime in Tiraspol and interested external actors, most notably the Russian Federation, to influence political decision-making in the Republic of Moldova and maintain a high degree of strategic uncertainty in the region.

The cumulative impact of these threats manifests across several interdependent dimensions. *At the level of internal security*, the proliferation and circulation of illegal weapons amplify risks associated with organized crime, undermine the rule of law, and generate persistent social vulnerabilities. *In terms of regional stability,* the existence and operation of trafficking channels may contribute to fueling armed conflicts in neighboring states, including the war in Ukraine, thereby intensifying the strategic volatility of the wider Black Sea region. *From an international image perspective, the Republic of Moldova's association* with a potential hub of arms trafficking and military insecurity negatively affects its European integration trajectory and its relations with international partners, eroding trust and diminishing willingness for deeper cooperation.

In essence, the military-industrial complex in the Transnistrian region constitutes a systemic threat with simultaneous internal and external implications, which cannot

be ignored in contemporary analyses of European security. Its multidimensional character - military, economic, and political - renders it a persistent source of vulnerability both for the Republic of Moldova and for the regional security architecture.

To mitigate these risks, several strategic courses of action can be outlined, addressed both to the political leadership in Chișinău and to international organizations and partners involved:

- *Inventory and international monitoring of armaments*. Active involvement of the OSCE and other relevant international actors in a transparent and verifiable process of monitoring weapons and ammunition stockpiles, with particular emphasis on sensitive depots in the Transnistrian region.
- *Strengthening border control.* Implementation of operational cooperation mechanisms with the European Union, based on advanced surveillance technologies, intelligence -sharing, and integrated inspection systems, aimed at reducing illicit flows.
- *Financial and economic control.* Identification and disruption of money-laundering channels linked to arms trafficking, alongside efforts to curb the region's parallel economy through financial, customs, and regulatory instruments.
- *Legislative and institutional reform.* Improvement of the national legal framework governing arms exports and dual-use goods, as well as the tightening of criminal sanctions for involvement in illegal schemes, in line with European and international standards.
- *Strategic communication and public diplomacy.* Systematic international exposure of illegal activities associated with the Transnistrian military-industrial complex, aimed at delegitimizing de facto structures and mobilizing political and technical support from external partners.

Accordingly, the military-industrial complex in the Transnistrian region is not a mere relic of the Soviet past but an active contemporary reality situated at the intersection of the military, economic, and political dimensions of insecurity. In the absence of effective and coordinated control and monitoring mechanisms, it continues to be a major source of instability for the Republic of Moldova and the broader Eastern European region.

Beyond the strictly military dimension, the issue under analysis also carries a profound human and societal dimension, as citizen security, social cohesion, and the prospects of European integration for the Republic of Moldova are directly conditioned by how this complex challenge is managed. The impact of threats posed by the Transnistrian military-industrial complex reverberates through internal stability and undermines the state's ability to construct a predictable security environment compatible with European standards.

The solutions identified are neither simple nor one-dimensional; they require coordinated international cooperation, coupled with sustained political will and long-term institutional perseverance. In this context, the analysis of the Transnistrian military-industrial complex goes beyond a purely academic endeavor, emerging as a practical and strategic necessity for safeguarding the national security of the Republic of Moldova and consolidating regional stability in Eastern European space.

A particularly relevant aspect requiring in-depth analysis concerns the activity of certain industrial enterprises located in the eastern part of the Republic of Moldova. Among the most notable are the enterprises "Pribor," "Metalorucav," "Kirov Electrical Appliances," the "Electromaș" industrial complex in the municipality of Tiraspol, as well as the metallurgical and hydraulic industrial complex in the city of Rîbnița. These economic entities, which officially operated under the guise of producing electrical appliances and household goods, were involved in illegal weapons production activities prior to the establishment of the European Union Border Assistance Mission to Moldova and Ukraine (EUBAM) (Cebotari 2023).

Available data indicate that the range of weapons illegally manufactured within these industrial complexes was diversified, encompassing both small arms and more complex weapons systems. Thus, weapons were clandestinely produced in the Transnistrian area, some of which were illegally traded in conflict zones such as Kosovo, Abkhazia, etc. (Sartori 2006). The types of weapons and ammunition illegally produced in the Transnistrian region are presented in Table 1.

These activities highlight the existence of an industrial infrastructure capable of sustaining the illegal production and distribution of weapons, with significant implications for regional and international security. In this context, a major strategic object is the Cobasna military depot, located near the city of Rîbnița in the northern part of the Transnistrian region. Covering an area of approximately 132 hectares, this facility has represented one of the largest storage sites for conventional weapons and ammunition in the post-Soviet space. According to available data, around 42,000 tons of weapons, ammunition, and military materiel originating from the former Soviet period were stored at Cobasna. The village of Cobasna is approximately 2 kilometers from the border with Ukraine, which further enhances its geopolitical and security relevance.

The ammunition depot primarily houses the armament legacy of the former 14th Army of the Soviet Union, as well as substantial quantities of military equipment originating from the former German Democratic Republic and Czechoslovakia. At present, more than 20,000 tonnes of ammunition are still stored within this perimeter. During the Soviet period, the Cobasna facility was known as Artillery Ammunition Depot No. 1411 and held the status of a strategic arsenal of the USSR's Southwestern Military District. A significant portion of the ammunition was transferred to and dismantled at this location after the withdrawal of Soviet troops from Central and

TABLE no. 1. Illegally produced weapons in the Transnistrian region of the Republic of Moldova

Weapon Category	Type/ Designation	Calibre/ General Characteristics	Platforme/ Use	Remarks
Multiple launch systems	Multiple launcher (20 tubes)	Not disclosed	ZIL131, Ural365 vehicles	Clandestinely produced; some units exported
Anti-tank launchers	SPIG-7	Anti-tanc	Man-portable	Illegal production
Anti-tank launchers	SPIG-9	Anti-tanc	Man-portable/ mountable	Illegal production
Mines	Artillery mines	82 mm, 120 mm	Artillery systems	Illegally manufactured
Mortar launchers	Katran	50 mm	Man-portable	Clandestine production
Small arms	PM revolver	9 mm	Individual weapon	Illegal production
Small arms	TT revolver	7,62 mm	Individual weapon	Illegal production
Small arms	PSM revolver	5,45 mm	Individual weapon	Illegal production
Assault weapons	AK-47 Kalașnikov	7,62 / 5,45 mm	Infantry	Multiple variants
Machine guns	Compact machine gun	9 mm	Infantry	Illegal production
Grenade launchers	Pcela	-	Man-portable	Illegally traded
Grenade launchers	Gnom	-	Man-portable	Illegally traded
Mortar systems	Vasileok	Vasileok	Vehicle-mounted	Some units were sold to rebel groups
Mobile launchers	Duga	-	Mobile	Illegal production
Grenade launchers	NPGM-40	40 mm	Mounted on AKS-74	Illegal production
Anti-personnel mines	PND	-	Ground-based/ wooden casing	Illegal production
Grenade launchers	GP-15	40 mm	Weapon-mounted	Illegal production

Source: Based on research conducted by the authors (Sartori 2006).

Eastern Europe, including the former German Democratic Republic, Czechoslovakia, and other member states of the former Warsaw Pact (Cebotari 2023, 122–127). The importance of this depot derives not only from the substantial volume of military stockpiles but also from its broader implications for regional security, geopolitical

stability, and the risks associated with the management, preservation, and potential neutralization of large quantities of obsolete ammunition (Digi24 2022).

As early as 2005, experts from the Academy of Sciences of Moldova (ASM) conducted a series of analyses and estimations based on available data concerning the composition, condition, and volume of ammunition stored on the left bank of the Dniester River. These assessments evaluated the potential risks posed by the long-term physical-chemical degradation of ammunition stored at the Cobasna military depot. According to the conclusions formulated by ASM specialists, under conditions of advanced degradation and an uncontrolled detonation, the energy released by an explosion could reach a level comparable, in terms of its destructive effects, to that of a tactical nuclear explosion. More specifically, the analyzed scenarios indicate that a potential explosion at the Cobasna depot could be energetically equivalent to the detonation of a nuclear bomb of approximately 10 kilotons, similar to the one used against the city of Hiroshima in 1945. This analogy is strictly comparative and illustrative in nature and is employed solely to highlight the potential magnitude of the effects of an accidental detonation of stored conventional ammunition, not to suggest the presence of nuclear materials at the site. At the same time, these assessments underscore the severity of the risks associated with maintaining massive quantities of ageing ammunition in an area characterized by high geopolitical sensitivity and in close proximity to densely populated localities (Timpul 2020).

A potential detonation of the ammunition depots could generate significant destructive effects on both the built environment and the population in adjacent areas. According to expert estimates, the resulting shockwave would be capable of destroying brick structures and reinforced concrete buildings located up to approximately 4–5 kilometers from the epicenter of the explosion (see *Figure* 2).

At the same time, a crater with an estimated radius of approximately 1.5 kilometers and a depth of up to 75 meters could be formed, indicating an extremely high level of released energy. Under the specific conditions of the Cobasna area, predominantly rural in character and characterized by relatively open terrain, the effects of the blast wave and the induced seismic vibrations could be felt over a much wider area, estimated at 40–50 kilometers. This would potentially affect settlements located at considerable distances, including the city of Orhei. From this perspective, the overall impact of such an explosion could be compared, in terms of its structural and geodynamic effects, to those generated by an earthquake with a magnitude ranging between 7.0 and 7.5 on the Richter scale. According to expert assessments, such an explosion would have severe consequences for the civilian population and would trigger a large-scale humanitarian and ecological catastrophe in the north-eastern region of the Republic of Moldova, with significant cross-border effects on Ukrainian territory. Depending on the scenario, the affected area could range between 500 and 3,000 square kilometers, influenced by the volume of ammunition involved and the physico-geographical conditions prevailing at the time of the event (Unimedia 2022).

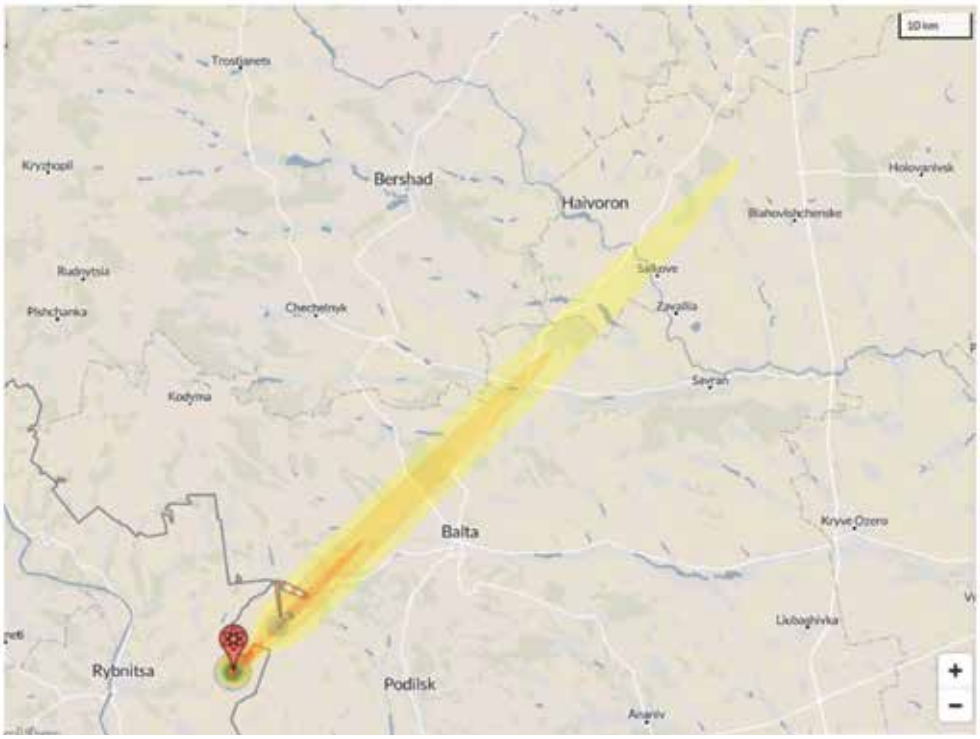

Figure 2 Simulation of the effects of detonation of a 10 kt nuclear charge (ground explosion) with the Cobasna center
Source: screenshot taken by the authors based on the detonation effects simulation application (NUKEMAP), accessed on 27.01.2026.

Thus, in the event of an accidental or deliberate detonation scenario, the associated risks are not confined to the strictly security-related dimension, but rather assume a complex, multidimensional character, with major implications for human security, regional stability, and environmental protection. The effects of a hypothetical scenario involving the detonation of a nuclear weapon with a yield of 10 kt TNT are presented in Table 2.

These data indicate that a nuclear-type detonation, even with a relatively low yield, would generate disproportionate systemic effects, simultaneously affecting human security, critical infrastructure, the environment, and regional stability, far exceeding the response and management capacities of a state the size of the Republic of Moldova. Such an eventuality would overwhelm the capabilities of local and national authorities, requiring coordinated international intervention, including in the fields of emergency management, humanitarian assistance, and long-term environmental damage assessment. In this sense, the continued existence of ammunition stockpiles in the Cobasna area represents not merely a material legacy of the Soviet military-industrial complex but also a structural vulnerability that reinforces the frozen character of the Transnistrian conflict and substantially complicates any effort toward a sustainable political settlement.

At present, the Russian Federation maintains approximately 20,000 tons of ammunition on the territory of the Transnistrian region, along with military

TABLE no. 2. Results of the simulation of the detonation of a nuclear weapon with a yield of 10 kt TNT (surface explosion) – Cobasna ammunition depot

Analytical dimension	Indicator	Technical Parameters	Estimated Impact / Interpretation
Scenario characteristics	Type of explosion	Surface nuclear explosion	Promotes soil radioactive contamination and extensive radioactive fallout
	Yield	10 kilotons of TNT	Comparable to tactical nuclear weapons
	Weather conditions (fallout)	Wind speed: 24 km/h	Spread accentuated in the wind direction
Direct human impact	Estimated deaths	~650 people	Majority in areas >5 psi and >500 rem
	Estimated injuries	~1.250 people	Mechanical trauma, burns, radiation exposure
	Population exposed to light blast (1 psi)	4.513 persoane /24 h	High risk of secondary injuries
Extreme thermal effects	Fireball radius	222 m	Total destruction of organic matter
	Fireball area	0.15 km²	Complete vaporization
Shockwave - Severe Damage	Overpressure	20 psi	Standard threshold for total destruction
	Affected radius	469 m	Structural collapse of reinforced concrete buildings
	Affected area	0.69 km²	Mortality near 100%
Shockwave - Moderate damage	Overpressure	5 psi	Threshold for major urban destruction
	Affected radius	0.99 km	Collapse of residential buildings
	Affected area	3.06 km²	Widespread injuries, multiple fires
Shockwave - Light damage	Overpressure	1 psi	Massive window breakage
	Affected radius	2.53 km	Frequent secondary injuries
	Affected area	20.2 km²	High number of injured
Acute radiological effects	Lethal dose (500 rem)	Acute exposure	Mortality within ~30 days
	Affected radius	1.25 km	High mortality
	Affected area	4.91 km²	Subsequent cancer risk (~15%)

Analytical dimension	Indicator	Technical Parameters	Estimated Impact / Interpretation
Thermal effects on population	Third-degree burns	≥8,44 cal/cm²	Full skin damage
	Affected radius	1.41 km	Permanent disability
	Affected area	6.22 km²	Requires major medical interventions
Radioactive fallout	1 rad/h contamination contour	98.7 km length; 7.46 km width	Extended regional contamination
	Affected area	~838 km²	Transboundary impact
	10 rad/h contamination contour	62.7 km; 4.48 km	Short-term dangerous doses
	Affected area	~386 km²	Severe access restrictions
	100 rad/h contamination contour	26.6 km; 1.5 km	Extremely dangerous doses
	Affected area	~104 km²	Uninhabitable
	1,000 rad/h contamination contour (stem fallout)	4.12 km; 0.82 km	Only column contamination
	Affected area	~5.29 km²	Not represented cartographically

Sursa: (NUKEMAP). The simulations were performed using the public application for modeling the effects of nuclear detonation, using standardized parameters and exclusively for analytical purposes.

contingents and associated infrastructure. In accordance with international commitments undertaken, these munitions and military forces were to be fully and unconditionally withdrawn from the territory of the Republic of Moldova by 2002, pursuant to the provisions of the Treaty on Conventional Armed Forces in Europe (CFE) and the Final Declaration of the 1999 Organization for Security and Co-operation in Europe (OSCE) Istanbul Summit (OSCE 1999). However, the withdrawal process was not completed. In 2007, the Russian Federation suspended its participation in the CFE Treaty and subsequently conditioned the full withdrawal of its munitions and troops on the political settlement of the Transnistrian conflict. This position contrasts with that of the authorities in Chișinău, which have consistently advocated for the total and unconditional withdrawal of foreign military forces and ammunition from the territory of the Republic of Moldova as a fundamental prerequisite for conflict resolution (Europa Liberă 2018).

A portion of the conventional armaments initially located in the region was withdrawn by the Russian Federation in previous years; however, there are indications

that some of these weapons may have been illicitly trafficked and sold to various regions of the world, raising additional regional and international security concerns. With regard to local military capabilities, the armed and paramilitary forces of the Transnistrian region comprise approximately 16,000 personnel, organized into four motorized infantry brigades, primarily deployed in Tiraspol, Rîbnița, and Dubăsari. These formations are equipped with modernized Soviet-era military equipment, including approximately 18 tanks, 107 armored vehicles, 73 artillery pieces, 46 anti-aircraft systems, and 173 anti-tank systems. The air component includes Mi-8T, Mi-24, and Mi-2 helicopters, as well as An-2, An-26, and Yak-18 aircraft. Officially, the Russian Federation declares the presence of around 1,200 military personnel in the area as part of the Operational Group of Russian Forces. However, in the context of the war in Ukraine, Ukrainian media outlets have advanced estimates suggesting that at least 5,000 Russian troops may be deployed in the Transnistrian region. This discrepancy between official figures and alternative assessments highlights significant transparency gaps and amplifies concerns regarding regional security stability (Cebotari 2023).

The analysis of external threats generated by the Transnistrian military-industrial complex cannot be separated from an assessment of the legislative and institutional framework governing the possession and circulation of weapons in the Republic of Moldova. Thus, national security is influenced not only by the existence of cross-border and geopolitical risks, but also by the state's ability to responsibly manage citizens' access to weapons and ammunition.

In the Republic of Moldova, the normative framework is regulated by the *Law on the Regime of Weapons and Ammunition for Civilian Use* (Legislative Portal 2012), which establishes the right to private ownership of firearms and related ammunition. According to official data from the State Weapons Register, approximately 69,400 lethal and non-lethal weapons subject to authorization are registered. Of this total, 396 legal entities own 5,231 weapons, while 55,464 private individuals own 64,169 weapons, including 19,467 rifled firearms, 41,932 smoothbore firearms, and 2,770 rubber-bullet pistols (Point 2015). According to the most recent police report, in 2024, approximately 81.6 thousand weapons were registered nationwide - an increase of 9% compared to 2023. Statistical data indicate that the number of residents of the Republic of Moldova legally owning firearms has increased, with nearly 65,000 individuals holding weapons lawfully, representing a 5% increase compared to 2024. The majority of these owners are aged between 35 and 50 years, including approximately 2,300 women (News Maker 2025). These figures illustrate a complex reality: although the legal regime is regulated and controlled, the overall volume of weapons circulating in the civilian sphere is significant. In the event of a crisis or armed conflict, this resource may become either a factor of security or one of vulnerability.

A particularly problematic aspect is that, in situations involving the declaration of a state of emergency, siege, or war, national legislation does not provide for a special regime

governing the use of weapons by lawful owners. In other words, current legislation establishes neither clear restrictions nor special rules for firearm holders under exceptional circumstances, potentially generating legal uncertainty and practical risks.

This gap becomes even more evident when examined in light of Ukraine's experience. In the context of the Russian Federation's invasion, Kyiv adopted the Law "On Ensuring the Participation of Civilians in the Defence of Ukraine" (Ligazakon 2022), which established a legal framework for the organized involvement of civilian volunteers in armed resistance. Confronted with the direct threat posed by the Transnistrian military-industrial complex and the risks associated with illegal arms trafficking, the Republic of Moldova requires a similar legislative approach, adapted to its national realities.

Accordingly, the issue of the weapons regime in the Republic of Moldova must be viewed in direct correlation with the risks generated by the Transnistrian military-industrial complex. While the Transnistrian region possesses a potential for the production and illicit trafficking of weapons, the Republic of Moldova already has a legal civilian base of weapons in circulation. In the absence of clear regulations for crises, a scenario may emerge in which legally owned weapons become sources of insecurity - through loss of control, theft, or secondary trafficking - or, conversely, are not effectively utilized as a defensive resource when national security so requires.

In this context, the following additional recommendations are proposed:

- *Amending legislation on the weapons regime,* by introducing clear provisions regarding the use of weapons by individuals and legal entities under exceptional circumstances (state of emergency, siege, or war).
- *Establishing a mechanism for integrating lawful weapons holders into the territorial defence system,* drawing inspiration from the Ukrainian experience while adapting it to the national legal and institutional framework.
- *Strengthening oversight of weapons holders*, alongside monitoring Transnistrian arms trafficking, through regular and rigorous verification of compliance with safety regulations by civilian owners.
- *Civic education and training,* including organizing training programs for legal holders to reduce accidental risks and prepare a responsible framework for the use of weapons.

Conclusions

The analysis of the military-industrial complex in the Transnistrian region, together with the large-scale storage of conventional ammunition and weapons in the Cobasna area, highlights the systemic and multidimensional nature of the risks involved, which extend well beyond the strictly military sphere and require an integrated approach encompassing diplomatic, information, military, and economic dimensions (DIME).

Diplomatic dimension. From a diplomatic perspective, the continued presence of Russian military forces and the maintenance of military-industrial infrastructure outside the constitutional control of the Republic of Moldova constitute an ongoing violation of the international commitments undertaken by the Russian Federation, including those within the OSCE framework and the conventional arms control regime. This situation undermines multilateral security mechanisms and erodes the credibility of the European arms control architecture. Strengthening diplomatic efforts, internationalizing the Cobasna issue, and revitalizing negotiation formats with the involvement of relevant international organizations remain essential for risk reduction and for identifying sustainable solutions.

Information dimension. In the information domain, the lack of transparency regarding the quantities, technical condition, and typology of stored weapons amplifies strategic uncertainty and facilitates disinformation at both national and regional levels. The absence of access for international observers and the lack of verified data create a permissive environment for the manipulation of security perceptions and the downplaying of real risks. The development of strategic communication mechanisms, supported by scientific expertise and independent assessments, is therefore necessary to underpin informed policy decisions and to properly inform the population about potential humanitarian and environmental consequences.

Military dimension. The military dimension remains the most visible and immediate component of risk. The storage of significant volumes of conventional ammunition—some of which has exceeded its service life—combined with the existence of clandestine weapons production and modification capabilities, increases the likelihood of accidental or deliberate explosions. The analyzed scenarios demonstrate that such an event could generate effects comparable to those of a major natural disaster or the use of a weapon of mass destruction, with severe consequences for the civilian population and critical infrastructure. In this context, the complete withdrawal of foreign troops, the demilitarization of the region, and the controlled neutralization of stored ammunition represent indispensable measures for mitigating military risks.

Economic dimension. From an economic standpoint, a major incident in the Cobasna area would generate extremely high direct and indirect costs associated with infrastructure destruction, agricultural land contamination, population displacement, and the management of a large-scale humanitarian crisis. The impact would extend beyond the borders of the Republic of Moldova, affecting regional economic chains and imposing substantial expenditures for decontamination and reconstruction. At the same time, the persistence of an illegal military-industrial complex distorts the local economic environment and fosters shadow economies and illicit arms flows.

Overall, the case of the military-industrial complex in the Transnistrian region illustrates the profound interdependence between the diplomatic, informational, military, and economic dimensions of security. Effective risk management cannot be achieved through isolated, sector-specific measures, but requires a coherent, multidimensional strategy oriented toward prevention, transparency, and international cooperation. The integration of the DIME framework provides the Republic of Moldova with an essential analytical tool for formulating coherent public policies aimed at safeguarding national interests and adapting to the regional security environment.

Finally, the case of the Transnistrian region underscores the need for further research into the interaction between frozen conflicts, military-industrial complexes, and national security, as well as for the development of specific policies to prevent the proliferation and accidental detonation of conventional weapons in sensitive regions.

References

Britanica. 2025. "Military-industrial complex." *Britanica*. https://www.britannica.com/topic/military-industrial-complex.

Cebotari, Svetlana. 2023. "The Transnistrian region of the Republic of Moldova in the context of the war in Ukraine." International Scientific and Practical Conference "Theory and Practice of Public Administration", May 20, pp. 122–127 https://ibn.idsi.md/sites/default/files/imag_file/122-127_29.pdf.

Digi24. 2022. "Transnistria susține că au fost trase focuri de armă dinspre Ucraina asupra depozitului de muniții al armatei ruse de la Cobasna." https://www.digi24.ro/stiri/externe/transnistria-sustine-ca-au-fost-trasefocuri-de-arma-dinspre-ucraina-asupra-depozitului-de-munitii-al-armatei-ruse-de-la-cobasna-1919373.

Dunne, J.Paul, and Elisabeth Sköns. 2009. "The Changing Military Industrial Complex." https://www2.uwe.ac.uk/faculties/BBS/BUS/Research/economics/The%20Changing%20Military%20Industrial%20Complex.pdf.

Europa liberă. 2018. "Adunarea generală a ONU cere Rusiei retragerea completă și necondiționată a trupelor sale din Republica Moldova." https: //moldova. europalibera. org/a/onu-moldova-rezolutie-retragerea-trupelor-ruse/29314184.html.

Financial Times. 2025. "Russia wants to deploy 10,000 troops in Moldovan breakaway region, PM warns." https://www.ft.com/content/c5a1faba-957c-4d5f-ac40-d126b643f07e.

Fiveable. 2025. "Military-Industrial Complex." https://fiveable.me/key-terms/apush/military-industrial-complex.

Global initiative. 2024. *Global Initiative Against Transnational Organized Crime. Smoke on the Horizon — Trends in Arms Traffic king from the Conflict in Ukraine.* Geneva: GI-TOC. https://globalinitiative.net/wp-content/uploads/2024/06/Smoke-on-the-horizon-trends-in-arms-trafficking-from-the-conflict-in-Ukraine-GI-TOC-June-2024.v3.pdf.

Koistinen, Paul A.S. 1980. *The Military-Industrial Complex: A Historical Perspective*. New York: Praeger Publishers.

Legislative Portal. 2012. "Legea nr.130 din 08.06.2012 privind regimul armelor și al munițiilor cu destinație civilă." https://www.legis.md/cautare/getResults?doc_id=17301&lang=ro.

Ligazakon. 2022. „Legea cu privire la asigurarea participării civililor la apărarea Ucrainei." https://ips.ligazakon.net/document/ view/T222114?an=1.

Mintz, Alex. 1985. "The military-industrial complex. American concepts and Israeli realities." *Journal of Conflict Resolution* 29(4):623-639. https://www.researchgate.net/publication/249728096_The_Military-Industrial_Complex.

National Archives. 1961. **"**President Dwight D. Eisenhower's Farewell Address." https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address?utm_source=chatgpt.com.

NewsMaker. 2025. "В Молдове растет число владельцев огнестрельного оружия." https://newsmaker.md/ru/v-moldove-rastet-chislo-vladelczev-orujiya-sredi-nih-bolee-2-tys-jenshin.

NUKEMAP. 2012. Aplicație utilizată pentru vizualizarea efectelor exploziilor armelor nucleare, creată de Alex Wellerstein. https://nuclearsecrecy.com/nukemap/#:~:text=Note%20that%20you%20can%20drag%20the%20target,more%20about%20the%20nuclear%20past%20and%20present%2C.

OSCE. 1999. *Declarația Summit-ului de la Istanbul 1999.* pp. 50-51. https: //www. osce.org/sites/default/files/f/documents/6/5/39569.pdf.

___. 2024. "OSCE strengthens Moldovan law enforcement'scapacity to combat illicit trafficking, with a focus on small arms and light weapons." https://www.osce.org/arms-control/577091.

Oxford. 2001. *Dicționar de politică.* Univers Enciclopedic. București.

Peterka-Benton, Daniela. 2012. *Arms Trafficking in Transnistria: A European SecurityThreat?* Montclair State University. https://digitalcommons.montclair.edu/justice-studies-facpubs/79.

Point. 2015. "Câți deținători de arme legali sunt în Republica Moldova." https://point.md/ru/novosti/obschestvo/catzi-detzinatori-legali-de-arme-sunt-la-moment-in-republica-moldova/?desktop=1.

Portal legislativ. 2012. "Legea nr.130 din 08.06.2012 privind regimul armelor și al munițiilor cu destinație civilă." https://www.legis.md/cautare/getResults?doc_id=17301&lang=ro.

Reaching critical will. 2025. "Military-industrial complex." https://www. reachingcriticalwill.org/resources/fact-sheets/critical-issues/6738-military-industrial-complex.

Roland, Alex. 2001. "Delta of Power: The Military-Industrial Complex." https://history.duke.edu/books/delta-power-military-industrial-complex.

Salisbury, Emma. 2024. "Beyond the Iron Triangle: The Military-Industrial Complex as Assemblage". https://eprints.bbk.ac.uk/id/eprint/53871/.

Sartori, Paolo. 2006. "La Transnistria chiave del Caucazo?" *Rivista italiana di Geopolitica* no. 6. Roma: L'Espresso. https://www.limesonline.com/rivista/la-transnistria-chiave-del-caucaso-14611290/.

Timpul. 2020. "Ce fel de muniții se află în depozitul de la Cobasna?" https://timpul.md/articol/ce-fel-de-munitii-se-afla-in-depozitul-de-la-cobasna-159067.html.

Țăranu**, Mariana.** 2024. *Regiunea separatistă de la Tiraspol-entitate rusă la hotarul Uniunii Europene. Panorama postcomunismului în Republica Moldova.* Institutul Cultural Român. București, V.I, p.169-214.

Unimedia. 2022. "Pericolul de la Cobasna: În caz de deflagrație, puterea exploziei ar putea echivala cu cea a unei bombe atomice, aruncată pe Hiroșima." https://unimedia.info/ro/news/c310d0072e2328e4/pericolul-dela-cobasna-in-caz-de-deflagratie-puterea-exploziei-ar-putea-echivala-cu-cea-a-unei-bombe-atomicearuncata-in-hirosima.html.

Vocabulary. 2025. "Military-industrial complex." *Vocabulary.com Dictionary.* https: // www.vocabulary.com/dictionary/military-industrial complex.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Aspects of Hybrid Warfare in the Dynamics of Its Manifestation Forms and Action Mechanisms

Mihaela HUŞANU*

*Romanian Parliament – Chamber of Deputies
e-mail: mihaela85husanu@gmail.com
https://orcid.org/0009-0006-1275-3618

Abstract

This article examines hybrid warfare as the dominant form of contemporary conflicts, in the context of profound transformations of the international security environment and the intensification of strategic competition among Great Powers. Starting from the evolution of war generations, from conventional to information confrontation, cyber and societal conflicts, the study highlights how hybrid warfare combines military and non-military instruments so as to produce strategic effects without triggering an open armed conflict. The main forms of manifestation of hybrid warfare at the diplomatic, political, economic, social, information, cultural, cyber, and non-military levels are analyzed, as well as the methods and tools used by hostile entities to render target states vulnerable. Methodologically, the article is based on specialized literature in the military, security studies, and international relations fields, the predominant approach being specific to qualitative study. The research conclusions reveal the need to emphasize the sociological dimension of the perception of hybrid threats among the civilian population. In the case of a hybrid war, strengthening the response capacity does not depend exclusively on military instruments, but on the level of knowledge, security education, and social cohesion, essential elements for the adaptation of states, especially in Eastern Europe, to the new paradigms of modern conflict.

Keywords:
Hybrid Warfare; Fifth Generation Warfare; Hybrid Threats; Impact; Russian Federation; Societal Resilience.

Article info
Received: 28 January 2026; Revised: 6 February 2026; Accepted: 13 March 2026; Available online: 8 April 2026

Citation: Huşanu, M. 2026. "Aspects of Hybrid Warfare in the Dynamics of Its Manifestation Forms and Action Mechanisms." *Bulletin of "Carol I" National Defence University* 15(1): 194-219. https://doi.org/10.53477/2284-9378-26-12

Motto: "States can potentially lose a war before even knowing that it has already begun." (Cholpon Abdyraeva)

Introduction

The main characteristic of the current international security environment, where antagonistic forces spread and interact, representing state and non-state actors projecting their power, is unpredictability. Considering the accelerated development of new technologies, which influence the world across all aspects, in a direct and still difficult-to-quantify manner, we are witnessing an intensification of strategic competition, in which geopolitical players come to prominence, pursuing opportunities and avoiding risks. From this perspective, the tense relations in the global geopolitical ecosystem develop because of a permanent update of the context of action, of the methods and instruments through which security threats are launched and responded to.

Thus, the physiognomy of conflicts tends to slide, as indicated by the new realities of the security environment, towards a sharp hybridization of the forms of confrontation. The frequent use of the concept of "hybrid war", especially after the invasion of Ukraine by the Russian Federation (2022), marked the moment of its transition from the sphere of military literature and security studies to the spectrum of public, political, and media discourse. Although it contributed substantially to the popularization of the term, this transition generated, at the same time, the risk of diluting its meaning through broad, imprecise, and superficial approaches.

This study aims to outline a relevant and multidimensional analytical framework for understanding the concept of "hybrid warfare" as an instrument capable of determining changes in the balance of power in the contemporary security environment, through the complexity of its forms of manifestation and the variety of specific action mechanisms. This approach is intended to bring more clarity regarding the nature, scope, and intensity of the threats generated by hybrid warfare, especially for decision-makers at the administrative and political level, for whom the ambiguities circumscribed to the topic represent obstacles in the substantiation and development of coherent public policies, adapted to the global context of instability.

At the same time, this analysis proposes a type of structured qualitative research on how the intensification of strategic competition among great powers influences hybrid warfare manifestations and generates an increased need to strengthen societal resilience. Societal resilience can be strengthened by examining not only perceptions, discourses, and institutional and social practices regarding non-military threats (disinformation, economic pressures, cyber-attacks, instrumentalization of social vulnerabilities), but also the mechanisms through which democratic societies can prevent, absorb, and respond effectively to new forms of conflict without eroding

their social cohesion, fundamental values , and public trust. In order to formulate flexible strategic responses, it is necessary, however, to crystallize a definition of hybrid warfare, explore the multiple dimensions at which hybrid threats operate, and understand the subtle phenomenon designed to exploit national vulnerabilities, while remaining below the threshold of detection.

The research objectives aim to clarify the concept of "hybrid warfare", through the comparative analysis of the main approaches in the specialized literature related to the military field, security studies and international relations, identifying the main forms of manifestation and mechanisms of hybrid warfare aggregated in the global environment, examining how the Russian Federation's pattern of action influences the Euro-Atlantic security architecture, as well as assessing the need to integrate and strengthen the role of the "education - societal resilience" binomial in security strategies, given that asymmetric threats constantly test social cohesion.

In order to achieve these objectives, the study is guided by the following research questions: "How has hybrid warfare emerged as the dominant form of contemporary conflicts, in the context of the transformations of the international security environment and the evolution of war generations?" "What are the main characteristics of hybrid warfare, and in what types of associations do these characteristics allow for the achievement of strategic effects without triggering an open armed conflict?" "To what extent do societal resilience and the perception of hybrid threats among the civilian population influence the capacity of states, especially those in Eastern Europe, to respond effectively to hybrid threats?"

Relying largely on secondary data from the specialized literature, on the content analysis of strategic documents, and on findings from comparisons of different theoretical approaches to hybrid warfare, this research is subject to inherent limitations characteristic of predominantly qualitative approaches. The subjectivity involved in the selection of the scientific resources consulted and in the interpretation of the in-depth perspectives of the analyzed authors constitutes a significant threat to the validity of the research. On the other hand, some limitations derive both from the restriction of the analysis to the non-linear warfare strategy of the Russian Federation, with few references to the hybrid warfare models used by other state or non-state actors, and from the complexity and dynamism of the explored phenomenon, which continuously adapts to geopolitical and technological transformations.

The conclusions of this analysis capture a specific stage in the evolution of contemporary conflicts, requiring an update that integrates further conceptual developments or additional theoretical approaches. Despite the limitations, the study provides a useful analytical framework for understanding hybrid warfare and can constitute a starting point for future research, including quantitative research.

Hybrid warfare, the archetype of contemporary war

The shaping of military war strategies has evolved in parallel with the complex transformations of the world, each stage being closely linked to the way in which power, technology, and social organization have been understood and used.
War can be defined, as Bărbulescu (2001) mentioned, as "the most violent form of manifestation of social conflict between large groups of people (states, groups of states, peoples, nations), organized from a military point of view, that use armed struggle to achieve political goals, thereby giving the phenomenon a distinctly destructive character.

The first generations of warfare reflected a world of emerging nation-states and symmetrical conflicts: the first generation, centered on large human mass, aimed at wearing down the opponent through confrontation, while the second generation shifted the emphasis from the power of firearms and artillery to the domination of the battlefield, through industrial superiority and the ability to concentrate "steel on the target". With the acceleration of mobility and complexity of political and economic systems, the third generation of warfare introduced maneuver as a central principle, aiming at the avoidance of the opponent's strengths and generalized collapse. In a world increasingly marked by fragmentation, non-state actors, and prolonged conflicts, the fourth generation of warfare shifted the center of gravity from military force itself to political and social will, through asymmetric and insurgent warfare (Neculcea 2020, 315). Currently, fifth-generation warfare is "dominated by non-kinetic actions, to the detriment of kinetic ones, by high technologies, to the detriment of classical, conventional means" (Popescu 2021), and the objective is no longer the physical destruction of the opponent, but subversion and cognitive manipulation.

Taken together, the fourth and the fifth generations of warfare reveal that, in a deeply interconnected and computerized global environment, forms of conflict tend to take on a predominantly hybrid character, primarily determined by the desire of great powers to avoid direct military confrontation, which involves major risks and high costs (Hoffman, Neumeyer, and Jensen 2024). The result is the transformation of conventional wars into an accumulation of political, economic, information, cyber, and limited military pressures, designed to produce strategic effects without triggering an open conflict. This trend places the international system in a turbulent and dangerous state, characterized by strategic ambiguity, gradual escalation, and the difficulty of clear demarcation between peace and war, a reality that challenges both deterrence mechanisms and the management of long-term security risks.

Introduced in the field of military theory, specialized literature to characterize the complex nature of the conflict between Israel and Hezbollah (2006), the concept of "hybrid warfare" designates the combination of conventional and unconventional

means of confrontation. In this conflict, the Lebanese non-state actor Hezbollah managed to combine conventional and unconventional tactics, modern military means, and guerrilla actions to counter a technologically superior military force. The decentralized organization, the use of autonomous cells, and the exploitation of the urban environment allowed for significant losses and revealed vulnerabilities of the Israel Defense Forces (IDF). The group effectively integrated the military with the political and information dimensions, using advanced weaponry (guided anti-tank missiles, operational and tactical missiles, drones, anti-ship missiles, and radio surveillance equipment) and techniques adapted to densely populated spaces (Potîrniche and Petrescu 2019).

Military history abounds in relevant examples of the use of conflict forms that can be retrospectively classified as hybrid warfare, characterized by the combination of conventional capabilities, subject to classical military rules and norms, with unconventional elements involved in irregular actions. From the Peloponnesian War, fought between the Spartans and Athenians, in the period 431 - 404 BC, the Jewish revolt of 66 AD against the Roman legions of Emperor Vespasian, to the Spanish-Portuguese War of 1807 - 1814 or "Operation Barbarossa" of the invasion of the Soviet Union by the Axis forces, during the Second World War (1941), the advantages of using unconventional actions were exploited together with conventional means of combat and contributed significantly to achieving decisive effects.

Some theorists argue that hybrid warfare, as described in many episodes in history, involves non-standard forces: local auxiliaries, militias, partisans, sabotage, and insurgency tactics. Their use allows a state not only to know better the battlefield, but also to have additional room for maneuvering, especially in expeditionary operations. Anglo-Saxon literature calls this type of warfare "compound warfare", and examples can be found in the French support for the American insurgents (1778 - 1781), the cooperation between Wellington and Spanish guerrillas against Napoleonic troops, and the cooperation between Napoleonic troops and auxiliaries (1809 - 1814).

However, other theorists use the phrase "hybrid warfare" to describe the appropriation, by non-state groups engaged in guerrilla warfare or terrorism, of advanced technologies. These technologies were originally designed for state forces but have been able to offer non-state actors increased firepower, as well as greater freedom of maneuver (portable anti-tank and anti-aircraft missiles, night-vision goggles, and other tools that have allowed the erosion of the comparative advantages of conventional forces).

The specialized literature uses diverse terminology to describe the concept of "hybrid warfare", which reflects an adaptation of the analytical interpretation framework to different strategic and cultural contexts. The Chinese strategic approach, formulated in the theory of "unlimited war", legitimizes the use of any instrument of power as

a means of influence. In the Anglo-Saxon approach, the term "hybrid warfare" has been established as a concept that synthesizes the convergence of a wide spectrum of risks, generated by adversaries who use military and non-military means. In contrast, the Russian approach operates with the term "non-linear warfare", which emphasizes the indirect, progressive, and integrated nature of actions carried out in the political, information, and societal fields, as essential elements of contemporary confrontation. All these concepts are related, emphasizing the plurality of perspectives on the forms of manifestation and mechanisms of action of hybrid wars.

1999 is the year that marked an important change in the way of understanding the conflict, in which the confrontation extends beyond the strict military sphere, with the emergence of the concept of "unlimited war", introduced in the work "War without restrictions", belonging to the officers of the Chinese People's Liberation Army, Qiao Liang and Wang Xiangsui. The authors supported the idea that any instrument at the disposal of a state or non-state actor can be used for conflict purposes, regardless of whether it belongs to the military, political, economic, or cultural domain. From this point of view, diplomatic actions, financial pressures, information manipulation, media influence, or exploitation of technological vulnerabilities were considered as relevant as the use of armed force. Thus, unlimited war is shaped as a continuous, diffuse, and potentially adaptive process, in which strategic competition takes place simultaneously on multiple levels, without respecting pre-established rules and without being conditioned by a formal declaration of war.

In the United States of America, the foundation of the "hybrid warfare" concept was laid by analyst Nathan Freier, one of the authors of the 2005 U.S. National Defense Strategy. The document signaled the transformation of the security environment and the convergence of traditional and unconventional threats (catastrophic and disruptive hi-tech terrorism), the U.S. increased exposure to these new types of threats to international stability, requiring a mandatory adjustment of the security response to hybrid forms of confrontation (Popescu 2014).

In 2007, American journalist and defense scholar Frank Hoffman conceptualized hybrid warfare as a complex form of conflict that combines multiple types of confrontation, from conventional military capabilities to irregular tactics and structures. This form of warfare includes the use of terrorism, with indiscriminate acts of violence and coercion mechanisms, as well as criminal activities designed to cause instability (Wither 2020). Such actions can be simultaneously carried out by both state actors and a diverse range of non-state actors, blurring the traditional boundaries between war, crime, and terrorism.

With the blurring of the boundary between peace and conflict, the security space is transformed into a profoundly unpredictable environment, difficult to manage through traditional means of defense. 5GW marks a paradigm shift because the protagonists of contemporary conflicts are state and non-state actors: "the battlefield is represented

by the entire society of the enemy, and the goal is, rather, the internal collapse of the enemy and not its physical destruction" (Lind 1989, cited in Neculcea 2020).

The hybrid threat was defined in 2009, at the U.S. Joint Forces Command hybrid war conference in Washington, as "any adversary who, adaptively and simultaneously, employs a combination of conventional, irregular, terrorist, and criminal means or activities in the operational environment. This adversary is a combination of state and non-state actors, rather than a single entity" (Potîrniche and Petrescu 2019).

Faced with hybrid warfare rewriting global security, the European Commission proposed a first definition of hybrid threats in 2016, characterizing them as "coercive and subversive activities, using conventional and unconventional methods (e.g. diplomatic, military, economic, technological), that can be used in a coordinated manner by state or non-state actors to achieve specific objectives, but remaining below the threshold of an officially declared state of war. The emphasis is usually on exploiting the vulnerabilities of the intended target and generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, which use social media platforms to control political discourse or to radicalize, recruit and coordinate intermediary actors, can constitute vectors of hybrid threats" (European Commission & High Representative of the Union for Foreign Affairs and Security Policy 2016).

What distinguishes contemporary warfare from previous generations of warfare is that it resides in a form of confrontation which combines conventional with irregular, economic, energetic, cyber, identity, and proxy warfare, in a complex, fluid, and unstable architecture, without limits and without restrictions. Insurgency, terrorism, and information warfare coexist in the same operations theatre because, according to the realist approach of the Italian Renaissance diplomat Niccolò Machiavelli, in war "tous les coups sont permis" (all blows are allowed) and the end justifies the means.

States with major military powers status, such as the USA, the Russian Federation, China, or France, are constantly reorganizing and adapting their military structures, orienting them towards the integration and development of capabilities specific to the conduct of offensive actions in cyber and space environments. This evolution reflects the recognition of the digital and space domains as new dimensions of armed confrontation, characterized by a high degree of interdependence with the land, air, and naval domains, as well as by their potential to generate disproportionate strategic effects.

The attacks on the Pentagon and the World Trade Center (USA, 2001) are examples of operations of unspeakable cruelty, as part of a campaign conducted in accordance with the principles of new generation warfare. They have forever dispelled the idea that contemporary warfare is only "terrorism" or something that happens solely in poverty-stricken third-world countries. 5GW is an unconventional form of warfare in which military force plays a much smaller, although still critical, role

than in previous generations, often in support of political, diplomatic, or economic initiatives. As important as finding and effectively destroying opponents is obtaining and consolidating a base of popular support (which questions the legitimacy of the target state government), which allows combatants to plan and execute their attacks.

Although from a tactical point of view the physiognomy of war has changed and adapted to the characteristics of the historic period in which the conflict took place, it has remained, in its essence, purely Clausewitzian, namely an instrument of politics. The historian and military theorist Carl von Clausewitz (1780 - 1831) spoke of war as "a continuation of politics by different means", and 5GW makes the concrete transition to this reality, with the complete fusion between the two principles, politics and war.

The role of advanced technologies in achieving victory in fifth-generation wars is decisive, as eloquently illustrated by the second Nagorno-Karabakh war, fought in the fall of 2020, between Azerbaijan and Armenia. The conflict demonstrated that military superiority is no longer determined exclusively by the size of conventional forces or classical territorial control, but by the coherent integration of advanced technological systems into the operational architecture, which acts as a force multiplier. The extensive use of reconnaissance and attack drones, loitering munitions, real-time surveillance systems, and electronic warfare capabilities allowed Azerbaijan to gain a significant information and operational advantage (Popescu 2021). This war also highlighted the importance of information integration, decision speed, and synchronized action in physical, information, and cognitive spaces, defining features of fifth-generation warfare.

Hybrid Warfare, a Component of the Russian Federation's Power Strategy

The "hybrid" dimension of war, a topic that has been intensely debated by the defense and security community, is not an absolute novelty. Over time, weaker adversaries have tried to identify and exploit to the maximum the vulnerabilities of stronger opponents and have done so countless times without considering rules, norms, or morality. "Victory can be created," said Sun Tzu, half a millennium BC, in his work "The Art of War". For this, the number of combatants and their strength are not enough, but skill, ability, capacity for analysis and synthesis, and the creative initiative that allows finding solutions to counter the adversary´s superiority in situations of asymmetry.

The concept of "hybrid warfare" gained increased theoretical relevance in the specialized literature since the middle of the last decade, especially because of the actions taken by the Russian Federation in Crimea, resulting in the annexation of the peninsula in 2014, as well as the military intervention in Syria, initiated in 2015.

As a particular form of non-linear conflict, hybrid warfare is associated with the Russian Federation's strategy of challenging the Euro-Atlantic security architecture and reconfiguring the spheres of influence in its strategic proximity, with reference to the historic spaces of Tsarist and Soviet domination. In this context, the Kremlin has developed and adapted a set of multidimensional strategies aimed at ensuring the expansion of its control capacity over the global geopolitical environment, including maritime, information, and strategic spaces, with the objective of asserting a hegemonic position in the international system.

The annexation of Crimea (2014) and the Russian invasion of Ukraine (2022) have validated the darkest fears, namely the return to a conflictual, anachronistic, 19th-century nature of warfare, while the means of waging war acquire extremely versatile valences: "vast geopolitical spaces are about to succumb to the flames of sectarian and religious conflicts, while supremacy for resources and economic influence pits the most prominent centers of power on the front line" (Bălăşoiu 2017, cited in Hornea 2017).

Revealing for understanding the Russian strategy and for deepening the risks associated with hybrid warfare are the directions indicated in 2013 by General Valery Gerasimov, Chief of the General Staff of the Russian Federation, strategic directions that substantiated what would later be the "Gerasimov doctrine". The rules of war themselves have changed, Valery Gerasimov specified, arguing that the role of non-military means in achieving political and strategic objectives has increased and, in many cases, these means are more effective than the power of arms. The methods applied in a conflict are more focused on bringing the target state to collapse through internal revolution and will emphasize "the integrated, large-scale application of political, economic, diplomatic, information, humanitarian and other non-military measures, in full correlation with the potential for revolt and protest of the population" (Eremia 2018).

The typology of the "Russian New-Generation War" described by Gerasimov integrates the armed forces with all other instruments of national power, using both conventional and unconventional forces, all equipped with cutting-edge technologies, the result being "total war". His strategic hypothesis starts with the idea that, in the 21st century, at a global level, there is a permanent state of conflict, with a tendency to blur the demarcations between war and peace. Moreover, the way wars are conducted has changed; wars are no longer formally declared, and after they are triggered, developments become unpredictable. The unprecedented rate of change characterizes the contemporary operational environment, and the rapid transition of some states from relative stability to violent confrontations and civil war is not an abnormality.

Other essential aspects concern: prevalence of the use of non-military means to achieve political-military objectives, clandestine application of the military

instrument, involvement of military capabilities being officially assumed in the final phase of the conflict, after the achievement of the decisive conditions for definitive success, reduction of the adversary's potential for action, even if it is superior in terms of conventional capabilities, by affecting cognitive capacity and exploiting identified vulnerabilities.

In the version adopted by the Russian Federation, hybrid warfare is presented as a form of adaptation to the political - economic - military reality, an attempt to overcome the technological gap and the differences in the quantity and quality of conventional military capabilities between the North Atlantic Treaty Organization (NATO) and Russia. This approach involves the revitalization of Soviet concepts, such as reflexive control and deep operation (Kasapoglu 2015).

Reflexive control, a concept developed since the 1960s, refers to the act of providing a partner or adversary with especially prepared information that leads them to voluntarily make a decision that benefits the initiator of the action. In this way, the targeted entity is influenced to adopt a course of action that is advantageous to the opposing party, without being aware of it.

As for the deep operation (battle), this concept was developed by a group of officers led by Marshal Mikhail Tukhachevsky during 1920-1930. In the context of hybrid warfare, the implementation of the deep strike principle involves paralyzing the adversary´s vital institutions and systems. Thus, necessary conditions are created for unrestricted action in which elements will execute shaping or decisive interventions during various phases of the operation itself.

The theoretical dimensions of the concept of "hybrid warfare" are in a permanent dynamic, ensuring an epistemological reflection on the practical aspect of applying multidimensional strategies and tactics that have changed the paradigm of conducting contemporary warfare (Ioniță 2014). The concept was also mobilized by NATO to explain the Russian strategy, highlighting its option to employ forces without uniforms and badges that allow identification ("little green men"), the engagement of local allies ("proxy war"), the use of propaganda promoted by social networks or the reinterpretation of agreements or treaties (giving rise to the concept of "lawfare").

Russia, however, does not have a monopoly on this type of war. U.S. permanently uses mercenaries, the famous "private military contractors", a fact which allows for economies of scale and gives the Pentagon greater maneuverability (in Iraq, Afghanistan). Beijing sometimes uses maritime militias ("little blue men"), interpretations and reinterpretations of maritime law, including by appropriating islands under commercial pretexts, but by creating infrastructure that could be suitable for military installations.

There is also a very close connection between asymmetric actions such as terrorism, organized crime, drug and human trafficking, and actions taken to undermine the legitimacy of the government or local authorities and generate or amplify a crisis. Opium production in Afghanistan or organized crime groups in the Americas (especially in Mexico) are disruptive factors that support this theory, advocated by Frank G. Hoffman (2009).

The combination of standard and non-standard or conventional and unconventional tactics makes it possible to carry out large-scale land operations, but sometimes also naval (for example, those carried out by the "Tamil Tigers" in Sri Lanka, the most dangerous terrorist organization in the world by the number of victims, or by Al-Qaeda in the Arabian Peninsula), air and ballistic ("Tamil Tigers", Hezbollah), information. The process of professionalization of non-standard fighters allows them to carry out combined operations, including all the mentioned components. In this sense, hybrid warfare is not just a tactical bricolage but rises to the level of an operational maneuver (Briot 2020).

The definition of hybrid warfare presented in the North Atlantic Treaty Organization Summit Declaration (September 2014, Wales) refers to "a wide range of military, paramilitary and civilian actions, conducted overtly or covertly in a highly integrated manner". The definition reveals the quintessence of the phenomenon, specifying that hybrid threats are represented by adversaries (states, irregular non-state groups - insurgents, terrorists, guerrillas, and members of organized crime; hybrid groups

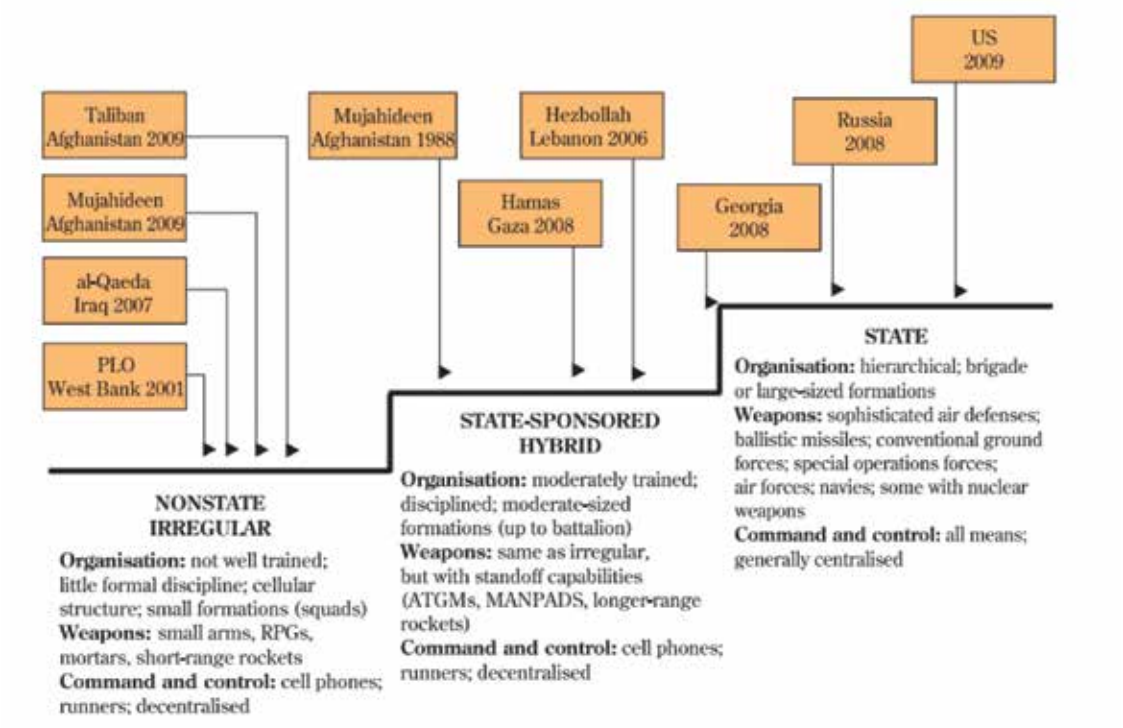

Figure 1 The Evolution of Hybrid Threats
Source: David Johnson 2009, RAND OP295-1

supported by states - Figure no. 1) who can simultaneously use conventional and unconventional means in order to achieve objectives.

Specific forms of manifestation and mechanisms of action

Certainly, in hybrid warfare, there are no longer separate threats with fundamentally different approaches. One can observe a convergence of irregular threats in which adversaries have a comprehensive, integrated approach to achieve their objectives. Hybrid threats target and influence a wide range of ways of waging war, combining conventional forces and capabilities with unconventional tactics and formations, subversive and terrorist acts that include generalized violence and coercion, destabilization of public order, and cyber-attacks.

Multimodal actions can be executed by separate structures, or even by the same unit, but are directed and coordinated in the operational space, at the operational and tactical levels, to obtain synergistic effects in the physical and psychological dimensions of the conflict. Consequently, the effects can be obtained at all levels of war: conventional, irregular, criminal, and cyber (according to Figure no. 2, which highlights the generic model of hybrid war).

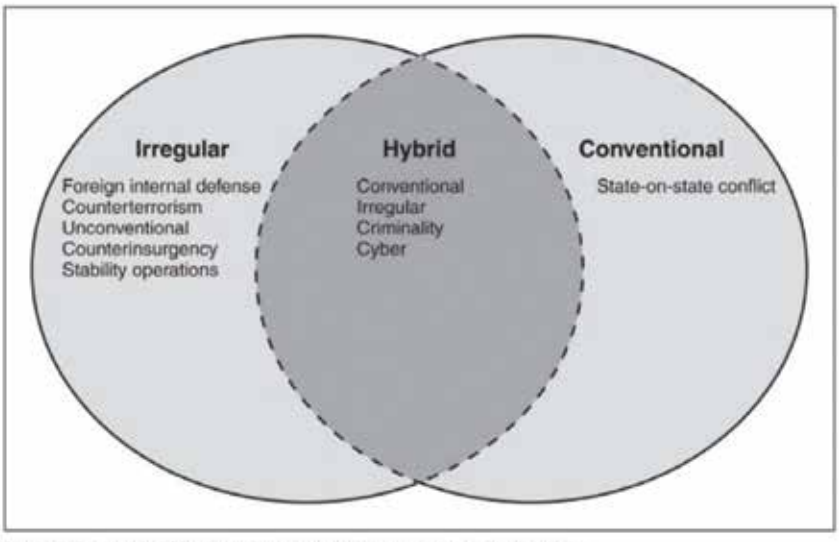

Figure 2 The Hybrid Warfare Concept

The diversity of forms in which hybrid warfare manifests itself is given by the multitude of areas in which asymmetric threats interfere: politics, diplomacy, culture, society, the rule of law, military and defense, outer space, administration, infrastructure, economy, intelligence, information, and cyber. These areas have been identified by the European Commission (EC) and the European Center of Excellence for Countering Hybrid Threats (Hybrid CoE) and are presented in the figure No. 3 (Source: https://euhybnet.eu).

Figure 3 The areas in which hybrid warfare operates

Clarifying the hybrid threat orchestration pattern are the methods used by the Kremlin to control the Great Planetary Ocean and ensure its global hegemony. These methods involve both military and non-military means, which will have repercussions in diplomatic, political, economic, information, cultural, cyber, and non-military terms, as Simileanu (2018a, 2018b) explains.

Hybrid warfare includes a distinct diplomatic dimension, in which the classical instruments of foreign policy are used primarily to undermine the existing international order and to advance the interests of the aggressor state without direct recourse to military force. From this perspective, diplomatic actions are oriented towards discrediting strategic competitors and reconfiguring international agendas in forums such as the United Nations or the Security Council, so that the attention of the international community is diverted from its own violations of international law. Relevant examples are the efforts to relativize or justify the annexation of the Crimean Peninsula by the Russian Federation and the constant diplomatic support granted to regimes under sanctions, such as the Syrian one, by blocking or diluting unfavorable international resolutions.

Russia's constant "reflexive control" campaigns demonstrate the Kremlin's concern to create narratives which seek to reinforce the perception – among Western countries and the Russian population – that it is an attacked state, responding in self-defense. Thus, alleged attempts to assassinate Russian President Vladimir Putin by the Ukrainian army are frequently invoked, and recently these practices have aimed to compromise diplomatic relations between Kiev and Washington, amid

negotiations to end the war in Ukraine. The Russian Ministry of Defense published on Telegram, in January 2026, a video showing the moment when the Chief of the Main Directorate of the General Staff of the Russian Armed Forces, Admiral Igor Kostyukov, hands an American attaché the control mechanism of a drone that he claimed was found among the fragments shot down at President Putin's residence in the Novgorod region (Saghin 2026). After Russia claimed that the residence had been targeted by an attack with 91 long-range drones, U.S. President Donald Trump initially took a favorable stance towards the Russian Federation, showing himself "very angry" about the alleged incident, and later qualified his position, sharing on social platforms an editorial from the "New York Post" that attributed responsibility to Russia for obstructing the peace process in Ukraine. Kiev denied that it carried out an attack targeting President Vladimir Putin, but the U.S. leader's reaction shows that the Russian tactic of shaping opponents through rhetoric and disinformation operations can produce temporary advantages for the Russian Federation by destabilizing Western decision-makers.

A central component of hybrid warfare is the use of regional conflicts and "peacekeeping" formats as levers of geopolitical influence. Involvement in frozen conflicts, such as those in Transnistria, South Ossetia, or the Donbas region, has allowed the aggressor state to simultaneously present itself as an interested party and an indispensable mediator, maintaining indirect control over the evolution of these files. In parallel, active participation in alternative or complementary multilateral formats to Western ones, such as BRICS, G20, G8 or the Shanghai Cooperation Organization, contributes to the consolidation of political and diplomatic support networks, often described as "clubs of friends" - according to the map in Figure No. 4 (Source: Anatoly Karlin), which can be mobilized to legitimize or defend controversial actions on the international stage - the "Club of Friends of Russia".

Last but not least, diplomatic hybrid warfare is also manifested through strategic involvement in negotiations and processes to resolve major international crises, to gain influence and control of dialogue channels. This is visible both in the role assumed in negotiations on regional conflicts, such as the one in Syria or attempts to position itself as a negotiator in the Ukrainian file, and in the involvement in sensitive discussions between other states, for example the negotiations between the United States of America and Iran or the support given to problematic nuclear programs, such as the North Korean one. Through such actions, the aggressor state not only consolidates its status as an indispensable actor but also manages to fragment collective efforts to combat global threats, from the proliferation of weapons of mass destruction to terrorism, drug trafficking, and organized crime, weakening the cohesion and efficiency of the international response.

At the political level, the Russian Federation's hybrid warfare is focused on practices through which it can maintain its dominant influence in the post-Soviet space, especially within the Commonwealth of Independent States, and extend this

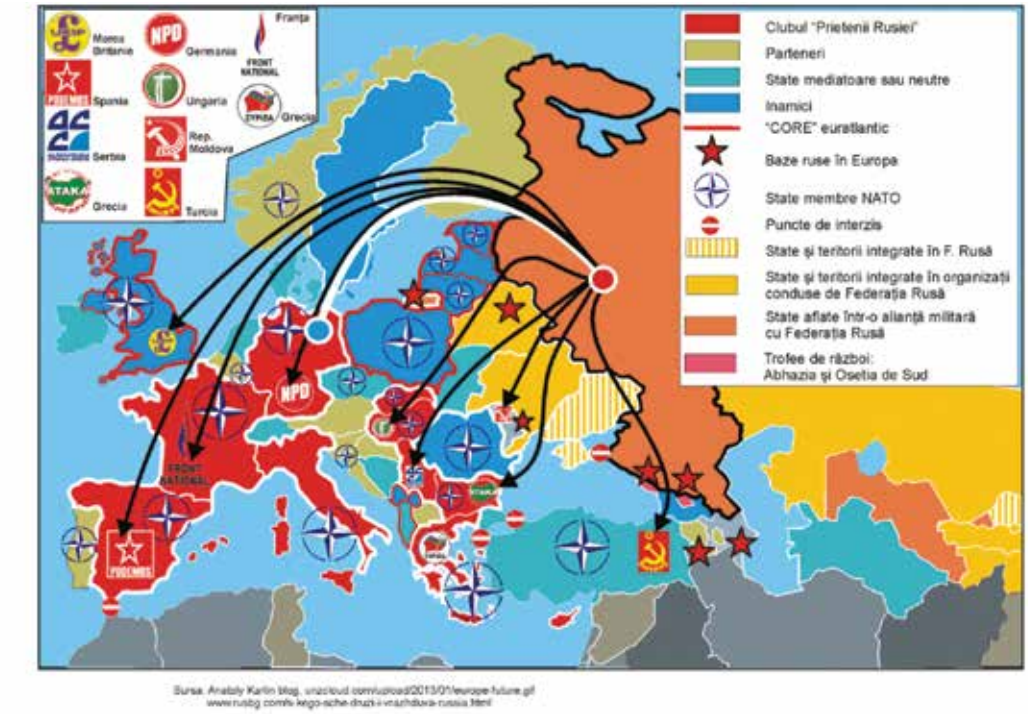

Figure 4 The "Club of Friends of Russia"

influence on Western states. In this sense, Russia capitalizes on the vulnerabilities already existing in Western societies. Social, economic, or identity problems are amplified and reinterpreted until they come to be perceived as major internal crises, capable of generating polarization and political instability. Nationalist rhetoric and patriotic discourse play an essential role in this process, being used to camouflage anti-Western messages and to undermine the legitimacy of the values and institutions that were the basis of European and Euro-Atlantic stability in the post-war period.

Another important component of this hybrid political strategy consists of exerting pressure on the European Union through strategic blackmail instruments, especially in the energy sector, and through capital controlled by oligarchic groups close to the Kremlin. In parallel, formal channels of dialogue with partners and allies are deliberately reduced or interrupted, while informal networks of influence, some built years ago, are reactivated and put to good use. These networks have also been used by involving top political actors from Western states, which has contributed to the erosion of internal consensus and the weakening of the cohesion of Euro-Atlantic alliances.

This type of hostile action aims to internally destabilize the target states. By heightening social tensions, cultivating collective fears, and deliberately stimulating feelings of hatred, radical political currents and extremist formations are encouraged, and they openly challenge alliances, treaties, and international institutions essential for the functioning of Western democracies. The support given to leaders of populist or far-right parties in Europe (for example, "Golden Dawn", "Jobik", "Syriza", "Patria", "Podemos", "National Front", "Ataka" or "Yukip), the use of former military

personnel or pensioners from the ex-Soviet space (Republic of Moldova, Latvia, Lithuania and Estonia) and the instrumentalization of sensitive areas, such as the Republic of Moldova, Ukraine or Crimea, as means of lateral pressure on Romania, Ukraine, Poland and Turkey, show this strategy´s methodical nature. Overall, the objective is not negotiation or cooperation, but induction of a climate of uncertainty and political chaos, intended to diminish the capacity of target states to coherently react to external influence and constraints.

The orchestration of hybrid warfare to have an impact at the societal level is based on recurrent discourses that call for the increased role of the social factor in the context of armed conflicts and local wars fueled by the Russian Federation. In fact, the policy of Russian President Vladimir Putin interferes with internal social strategies and creates development gaps compared to Euro-Atlantic states. Through Stalinist and neo-Soviet-style discourses, Putin has managed to "reanimate" the social sacrifice imposed by the arming of a non-existent enemy, permanently demonized. The result also consists of inducing insecure, national-defensive behavior at home, but also in diplomatic and international relations. Particularly important is the method of bringing the target state to collapse through internal revolution, a method that emphasizes the large-scale application of political, economic, diplomatic, information, humanitarian, and other non-military measures, in full correlation with the population´s potential for revolt and protest. Such operations have the potential to transform a stable political and social situation in a target state into a general state of chaos, bordering on the outbreak of civil war, which creates the premises for external intervention.

The economic dimension of hybrid warfare relies on the deliberate use of economic interdependencies as an instrument of influence and coercion. One of the constant objectives of the Russian Federation is to deepen the dependence of European states on Russian energy resources, especially gas, by expanding the transport infrastructure to Western markets and, simultaneously, by obstructing or delegitimizing alternative energy diversification projects. This strategy is supported by investments in key areas of the economy (banking, hospitality, professional sports, or information technology), which allow both secure access to capital and the exercise of indirect influence on economic and political decisions. Against the background of the economic pressure exerted, strategic advantages are obtained, and dependent states have limited room for maneuver.

To maintain energy dependence, Russia often resorts to explicit forms of coercion, illustrated by repeated episodes of interruption or conditioning of energy supplies in relations with Ukraine and Georgia. The practices known as "energy coercion" have direct effects on the targeted state's economic and political stability. In parallel, the hybrid war with economic implications includes the financing of anti-state structures (anti-Ukrainian in Crimea and the Donetsk-Lugansk area), pro-Russian NGOs in the ex-Soviet and ex-communist space, with main targets such as Poland,

Romania, and Turkey, and pro-Russian networks in regions such as Crimea, Donbas, Ukraine, the Republic of Moldova, or Georgia. These financial flows have the role of supporting the challenge to the state's authority, fueling internal tensions and creating economic dependencies that can later be exploited for political purposes.

Another pillar of the Russian strategy for implementing hybrid warfare is represented by cross-border money laundering networks, involving politicians, members of security structures, actors in the judicial system, banking institutions, and criminal groups, a strategy that has been documented both in the European Union and in the former Soviet states. Such practices have been complemented by the promotion of the Eurasian Customs Union, transformed into the Eurasian Economic Union as of January 1, 2015. Far from being just an economic integration project, this framework has functioned as an instrument for forcibly anchoring the participating states in an economic space dominated by the Russian Federation, reducing their decision-making autonomy and external strategic options.

At the cultural level, the hybrid warfare practiced by the Russian Federation is based on the use of identity, religion, and historic memory as tools of geopolitical influence, through "cognitive hacking" (Chifu 2018). A central element of this strategy is the promotion of a messianic discourse, which reinterprets older ideological traditions, such as pan-Orthodoxy and pan-Slavism, to legitimize contemporary geopolitical ambitions. These currents are reactivated as mechanisms of symbolic mobilization, intended to justify Russia's self-proclaimed role as "protector" of the Orthodox and Slavic world. In this context, references to the occupation of Constantinople and the control of the maritime constriction points of the Bosphorus and the Dardanelles acquire a clear geopolitical significance, being integrated into a discourse that combines religious, historic, and strategic elements to support objectives of regional influence (Figure No. 5).

Figure 5 Russian cultural space (GeoPolitica 2018)

In addition, this cultural strategy includes forms of symbolic aggression and the instrumentalization of existing identity tensions. By organizing cultural and academic events in the Euro-Atlantic space, which promote narratives favorable to Moscow, Russia aims to normalize alternative interpretations of political and economic realities in the context of major internal difficulties of the Russian Federation. At the same time, one can observe a tendency to resuscitate and exploit ethnic and religious conflicts by emphasizing identity differences and fueling historical resentments. These practices allow social cohesion fragmentation in the targeted states and favorable terrain for external influence, in which cultural identity becomes a vector of political pressure and long-term destabilization.

At the information level, hybrid warfare mainly acts in the online environment, especially on social media platforms, which provide a favorable framework for the use of asymmetric instruments of influence. The information space allows for low-cost, high-impact operations aimed at eroding social cohesion, diminishing trust in institutions, and weakening the response capacity of the targeted states. New digital technologies facilitate strategic influence operations, through which public perceptions are shaped with certain goals that serve the aggressor, and the potential for mobilization of the adversary is reduced without resorting to direct military confrontation. In this context, traditional press has also become a target, but differences in regulation, transparency of financing, and mechanisms for editorial accountability clearly delimit it from the opaque ecosystem of social networks.

A defining element of the mechanisms aggregated by hybrid warfare is the use of information manipulation techniques, which, from the perspective of the psychological impact pursued, show many similarities to the methods encountered in terrorist threats. Practices such as selection and truncation of information, biased framing of statements by political leaders, or presentation of opinions as indisputable facts are frequently used to build narratives favorable to the hostile entity. Media platforms affiliated with Russia ("Russia Today" or "Sputnik") are often associated with such strategies, complemented by the limitation of the right to reply in the domestic information space. Intentional overlap of factual statements and opinions, generalization of specific events, or selective omission of relevant international developments also contribute to distorting reality and inducing confusion among the public.

At the same time, the manifestations of information warfare are amplified by certain characteristics of social media platforms, where the lack of rigorous control over the identity of users and the dynamics of algorithms favors the proliferation of fake accounts, troll networks, and coordinated disinformation operations. Techniques such as the spread of fake news, imagological attacks on political leaders and international organizations, or the symbolic use of public shaming gestures have the role of undermining the morale of the targeted societies and eroding confidence in the prospects of success or stability. All these actions, carried out both through media

channels loyal to Moscow and through global digital platforms, configure a toxic information ecosystem in which disinformation, propaganda, and manipulation are central tools of contemporary hybrid warfare.

Beyond the classical military dimension, hybrid warfare is increasingly manifested through a set of non-military actions that target the vulnerabilities of modern societies. A central role is played by cyber-attacks, directed both against states and international organizations, as well as against financial and banking institutions or individual actors considered inconvenient (journalists, analysts, groups active in the online environment). These attacks do not exclusively aim to cause technical damage, but have as their main objective the intimidation, collection of information, and discrediting of independent sources of analysis. In parallel, ideological propaganda is strategically integrated into diplomatic and academic contexts or in high-visibility international events, where messages are calibrated to influence political and opinion elites.

Another level of these non-military manifestations is represented by the expansion of influence networks and the attraction of supporters through unconventional methods. Intelligence structures, digital social networks, and informal communities, including groups associated with ultras phenomena or online subcultures, are used to create loyalties and mobilization channels. Alternative financial instruments, such as cryptocurrencies, as well as global trading platforms, are exploited to facilitate discreet financing and coordination of actions. At the same time, sustained efforts are observed to co-opt or influence media trusts from the Western space, to legitimize certain narratives and amplify messages favorable to Russian interests within democratic societies.

At the same time, non-military hybrid warfare includes actions of symbolic denigration and discrediting. Cultural values in the historical territories of states that belonged to the former Soviet Union are frequently the target of delegitimization campaigns, designed to weaken national identity and social cohesion. Attacks on political leaders, often focused on their personal lives, are used to diminish public credibility and induce distrust (for example, the pro-Kremlin press constantly portrays Ukrainian President Volodymyr Zelensky as a "drug-addicted leader with worsening mental health problems") (Gherman 2025). These practices are complemented by campaigns to destroy the country's image and the use of extortion or non-transparent financing to support pro-Russian groups and influential individuals. Overall, these non-military instruments outline a broad strategy of pressure and destabilization, which aims to obtain political and strategic advantages without direct recourse to armed force.

At the cyber level, hybrid warfare exploits states' vulnerabilities with potential consequences both on national security and on the integrity of physical, digital, and financial assets. The aim is to gradually erode the functioning of essential public services and diminish the population's trust in the ability of state institutions to

ensure the protection of fundamental interests. Cyber interventions can take various forms, from the interruption of vital services and identity theft to the manipulation of control systems used in the management of critical transport infrastructures, with a direct impact on road, rail, or air traffic. In addition, there are attacks on IT security mechanisms and cyber espionage campaigns aimed at civilian and military servers of EU and NATO member states, as well as cybercrime activities aimed at obtaining financial benefits through illegal theft and exploitation of information.

The accelerated development of new technologies and the expansion of digital space have multiplied the tools available for hostile actions in the online environment. The Internet is used not only for propaganda and psychological warfare, but also for recruitment, mobilization, fundraising, and information collection through advanced data analysis techniques. Encrypted communication, coordinated cyber-attacks, and distribution of extremist content through mobile applications complete this spectrum of threats. In addition, advances in the field of artificial intelligence allow the generation of extremely realistic fake content, from the real-time manipulation of facial expressions and voices to the creation of synthetic images and audio-video materials or press articles built on data sets (polls, election results, financial reports) that can mislead public opinion.

All these developments highlight the fact that modern warfare is characterized by the simultaneous integration of several types of capabilities and instruments of influence. Cyber operations are correlated with information warfare actions, economic pressures, political and diplomatic approaches, as well as, in certain situations, with the use of special operations forces acting in connection with internal opposition groups in the target state. Depending on developments on the ground and the reactions of the actors involved, these actions are adjusted, coordinated, and permanently recalibrated, with the aim of maximizing efficiency and achieving the established strategic objectives, without exceeding the threshold of a direct conventional military confrontation.

Hybrid warfare and societal resilience

Through the complexity of integrated dimensions, as well as through the variety of tools and methods used, hybrid warfare involves society at large, subjecting it to a permanent test of cohesion while faced with asymmetric threats. Since the adversary acts at the limit of detection (in the "gray area"), and the methods of confrontation are marked by ambiguity and the lack of clear demarcations, the process of identifying risks and formulating responses becomes sinuous, favoring the amplification of vulnerabilities and their transformation into systemic crises.

The concept of "societal resilience" refers to "the capacity of communities to flexibly absorb major disruptions and to rapidly recover from the inevitable decline in basic functionality" (Elran 2017, cited in Lesenciuc 2024). The term implies the state´s

ability to protect its sensitive points, which may be perceived by hybrid actors as strategic opportunities, as well as to consolidate, rebuild, and adapt its critical infrastructure (made up of both tangible and intangible components) after the manifestation of a hybrid action.

Managing a hybrid war and all the effects that arise from its impact on society does not solely lie in the state´s power, with its entire network of administrative institutions. Countering hybrid threats also depends on citizens´ resilience, which is built over time, and its foundation is education in the spirit of defending national values and the nation itself. The effort must be conscious and convergent, with each citizen's reactions being guided by the feeling of strong identity, but also by the deep component of patriotism that animates society. In this sense, recognizing the education - societal resilience nexus is essential for any security strategy.

The hybrid war mechanism (according to Figure 6) acts on the territory of a state, defense forces, leaders and population predominantly with informational attack forces, so that societal resilience must be built in the sense of blocking the action of media and other instruments of influence on the psychology of the masses and "opaquing" distorted perception, through the bombardment with fake news and images regarding the events in progress.

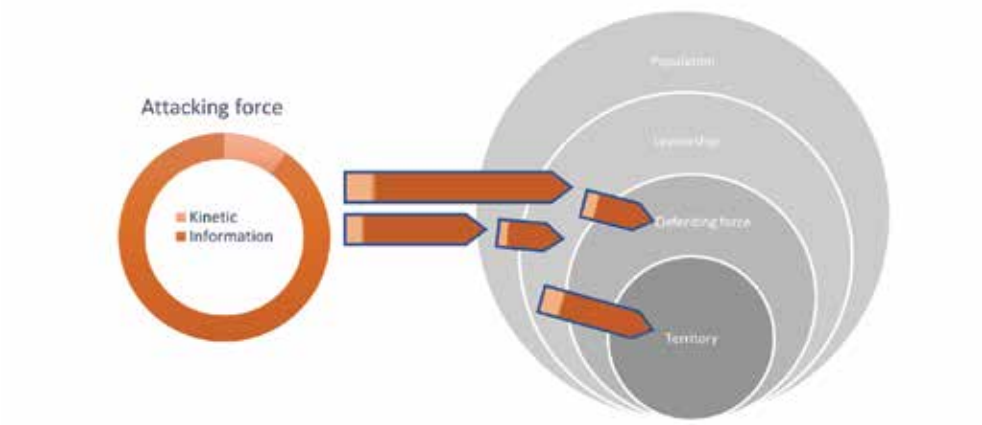

Figure 6 The mechanism of hybrid warfare
Source: Mînzărari 2020

In fact, public perception must be based on the image dimension of the state, the leadership, the political decision-maker, and the regime. Trust in these elements is mandatory, because on trust are built the ideas of national representation and the perspective of the development of the state and society, respectively the credibility of the leader and the state force, which induces a high level of hope at the individual and societal level.

One of the characteristics of asymmetric warfare is the continuous interaction, within the same confrontation, between the elements of hard and soft power, which are enhanced in strategic combinations adapted to the context, thus resulting in smart

power. While hard power represents the use of military force or the coercive capacity of a state, soft power cultivates compliance through a variety of policies, qualities, and actions, indirectly and through non-coercive measures. Hybrid warfare allows actors to operate in the shadow, at the border between war and peace, with both hard coercive instruments and soft instruments (e.g., propaganda and disinformation campaigns aimed at psychosocial destabilization), as a complex interface located at the meeting point between conventional and unconventional threats (Figure no. 7).

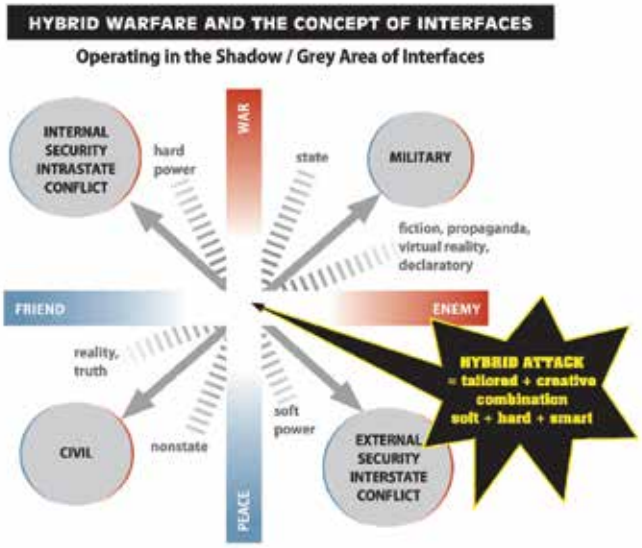

Figure 7 Hybrid warfare and the interface concept (NATO StratCom COE)

"A more resilient Europe, fully equipped to face today's complex and dynamic security threats" is also the aspiration of the European Union leaders, who are working to develop resilience and counter hybrid threats. In this regard, the European Commission is monitoring the overall implementation of the Joint Framework on Countering Hybrid Threats. The EU proposals aim, among others, at various means to develop capabilities and counter cyber threats, such as a mandate to strengthen and modernize the European Union Agency for Cybersecurity, a "blueprint" for cooperation between Member States and EU agencies in the event of an attack, and the cyber diplomacy toolbox. Moreover, "if 2025 was the year of recognition of Russia's hybrid threats, 2026 must be the year of response" (Bowser 2025).
On the other hand, the NATO 2030 Strategy mentions that, in the event of a hybrid war, the North Atlantic Council could decide to invoke Article V of the Washington Treaty, as in the case of an armed attack.

Conclusions

Hybrid warfare can be understood as the result of an evolutionary process of armed conflicts, generated by the dynamics of social, technological, and political transformations that characterize the contemporary international environment. Against the background of this evolution, the paradigm of conventional

confrontation, centered almost exclusively on the use of military force, has been progressively complemented by flexible forms of action, in which state and non-state actors simultaneously resort to military and non-military instruments. This expansion of the spectrum of means has contributed to a substantial redefinition of the concept of security, demonstrating that traditional military advantage no longer constitutes a guarantee of strategic success. The potential to correlate political, economic, information, and cyber pressures becomes, in this context, a determining factor of strategic efficiency.

The ongoing hybrid war of the Russian Federation constitutes a reference point in the analytical consolidation of this type of conflict, requiring a reassessment of the prevention and response tools used at the international level. The ambiguity of the actions of the Russian Federation, the coordination of military means (in Ukraine) with non-military ones, and the conduct of operations in several areas have significantly complicated the early identification of aggression and the articulation of a coherent response. Thus, the need to orient research on hybrid warfare towards institutional, sociological, and operational perspectives, capable of capturing the interdependence and complexity of this phenomenon that represents the main threat to the security of states in the 21st century, becomes imperative.

Strengthening societal resilience emerges as a central dimension of countering hybrid threats. Security requires not only the accumulation of military capabilities, but also an integrated approach, which includes security education, increasing public awareness, strengthening social cohesion, and adapting institutions to new risk patterns.

For Romania and for the Eastern European states, located in the vicinity of areas marked by instability, the development of flexible and multidimensional response mechanisms is a strategic necessity. Only through a coherent approach, which articulates the military with the societal and institutional dimensions, can contemporary hybrid conflicts be effectively managed, as expressions of the way in which the world is configured, interpreted, and contested.

References

Bărbulescu, I. 2001. "War and armed struggle. The content and general physiognomy of armed struggle." *Land Forces Academy Review* 2. https://www.armyacademy.ro/reviste/2_2001/c3.html.

Bârgăoanu, A., and E. Negrea-Busuioc. 2024. "Hybrid warfare is less than warfare: A dangerous illusion." *IW Perspectives* No. 19. https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf.

Bowser, D. 2025. "Russian organized crime and its links to hybrid warfare in Europe." GLOBSEC Report. https://www.globsec.org/sites/default/files/2025-12/Russian%20Organised%20Crime%20and%20Links%20to%20Hybrid%20War%20in%20Europe%20ver3%20web%20spreads.pdf.

Briot, T. 2020. *Hybrid warfare, the new nature of global conflicts.* https://truestoryproject.ro/razboi-hibrid-natura-conflictelor-mondiale/.

Chifu, I. 2016. *Hybrid war, "lawfare," information warfare. Wars of the future.* https://adevarul.ro/blogurile-adevarul/razboi-hibrid-lawfare-razboi-informational-1696690.html.

___. Chifu, I. 2018. "Hybrid warfare and societal resilience. Planning hybrid defense." *Infosfera. Journal of Security and Defense Intelligence Studies* Nr. 1: 28-30.

___. 2022. *Reconfiguring security and international relations in the 21st century.* Vol. 2: Threats and conflicts in the 21st century. Bucharest: RAO Publishing House.

___. 2025. "Conceptualization and epistemological assessment: Cognitive warfare." *Infosfera. Journal of Security and Defense Intelligence Studies* Nr. 2: 5-18. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2025/2_2025.pdf.

Eremia, C. 2018. „Innovative Russian approaches to modern warfare." *Monitorul Apărării și Securității.* https://monitorulapararii.ro/abordari-inovative-ale-rusiei-privind-razboiul-modern-1-4718.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. 2016. "Joint framework on countering hybrid threats: A European Union response." JOIN(2016) 18 final. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52016JC0018.

European Commission. 2020. "Communication on the EU Security Union Strategy." Bruxelles, pp. 14–20. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52020DC0605.

Frunzeti, T., and C. Bărbulescu. 2018. *National resilience to hybrid threats and security culture: An analytical framework.* https://www.aosr.ro/wp-content/uploads/2019/03/Anexa-1_Articol-Impact-Strategic-2018.pdf.

Gherman, M. 2025. *War propaganda: Zelensky is using drugs and is mentally unstable.* https://www.veridica.ro/fake-news-dezinformare-propaganda/propaganda-de-razboi-zelenski-se-drogheaza-si-e-instabil-psihic.

Hoffman, F. 2009. "Hybrid vs. compound war." *Armed Forces Journal.* http://www.armedforcesjournal.com/hybrid-vs-compound-war/.

Hoffman, F., M. Neumeyer, and B. Jensen. 2024. "The future of hybrid warfare." *Center for Strategic & International Studies.* https://www.csis.org/analysis/future-hybrid-warfare.

Hornea, I. 2017. "Hybrid warfare, a transitional stage toward the conflict of the 21st century." *Military Sciences Review* 4 (49): 77-93. https://aos.ro/wp-content/anale/R-S-M-Vol-17-Nr4Full.pdf.

Ioniță, C.C. 2014. „Is hybrid warfare something new?" *Impact Strategic* 4 (53): 64-76. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

Kasapoglu, C. 2015. „Russia's renewed military thinking: Non-linear warfare and reflexive control ." NATO Defense College Research Paper No. 121. https://www.ndc.nato.int/download/russias-renewed-military-thinking-non-linear-warfare-and-reflexive-control/?wpdmdl=7278.

Lesenciuc, A. 2024. "Societal resilience as intangible critical infrastructure." *Gândirea Militară Românească* Nr. 2: 94-109. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2024/2/LESENCIUC.pdf.

Libiseller, C. 2023. "„Hybrid warfare" as an academic fashion." *Journal of Strategic Studies* 46 (4): 858–880. https://doi.org/10.1080/01402390.2023.2177987.

Lupulescu, G.D. 2023. "Hybrid, defining the concept of war, operations, and threats of the 21st century." *Bulletin of "Carol I" National Defence University* 12 (2): 56-68. https://revista.unap.ro/index.php/revista/article/view/1713.

Marcuzzi, S. 2018. "Hybrid warfare in historical perspective ." [Paper presentation, Max Weber International Workshop, NATO Defense College Foundation]. https://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf.

Mînzărari, D. 2020. "Understanding 'hybrid warfare': A conceptual approach." *Institute for European Policies and Reforms*. https://ipre.md/wp-content/uploads/2020/12/Policy-Paper_Understanding-hybrid-war_Dumitru-Minzarari.pdf.

Neculcea, C. 2020. "Generations of warfare, conventional and unconventional in the evolution of wars." In *Proceedings of the International Scientific Conference „Gândirea Militară Românească"*, 310-317. https://gmr.mapn.ro/webroot/fileslib/upload/files/conferinta%202020/proceedings/neculcea.pdf.

Popescu, A.I.C. 2014. "Observations on the relevance of hybrid warfare. Case study: Ukraine." *Impact strategic* 4 (53): 124-148. https://cssas.unap.ro/ro/pdf_publicatii/is53.pdf.

___. 2021. "Observations on fifth-generation warfare and the Second Nagorno-Karabakh War." *Bulletin of "Carol I" National Defence University* 10 (4): 39-45. https://revista.unap.ro/index.php/revista/article/view/1297.

Potîrniche, M.T., and D. Petrescu. 2019. *Countering hybrid threats to state security: Specialized study.* București: "Carol I" National Defence University Publishing House. https://cssas.unap.ro/ro/pdf_studii/modalitati_de_contracarare_a_amenintarii_hibride.pdf.

Presidency of Romania. 2021. *NATO Brussels Summit communiqué.* https://www.presidency.ro/ro/media/comunicate-de-presa/comunicatul-summitului-nato-de-la-bruxelles-14-iunie-2021.

___. 2025. *National Defence Strategy of Romania for 2025–2030. Independence and solidarity, Romania's vision for a changing world.* https://www.presidency.ro/ro/media/csat/strategia-nationala-de-aparare-a-tarii-pentru-perioada-2025-2030.

Răpan, F. 2019. "Symmetry and asymmetry in current military conflicts." *International Scientific Conference „Gândirea Militară Românească.* Ministry of National Defence Publishing House. pp. 266–281. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/Conferinta%20GMR%202019/GMR_CONF%20ro_Rapan.pdf.

Saeed, A. 2024. "Fifth-generation warfare." *Defence Journal.* https://defencejournal.com/2024/04/08/the-5th-generation-warfare/.

Saghin, S. 2026. *Russia handed the U.S. evidence of an alleged Ukrainian attempt to attack Putin. Ukraine's response.* https://stirileprotv.ro/stiri/international/rusia-a-inmanat-sua-dovezi-despre-presupusa-tentativa-de-atac-ucrainean-asupra-lui-putin-cum-raspunde-ucraina.html.

Sciutto, J. 2025. *The return of great powers: Russia, China, and the next world war.* Bucharest: Corint Istorie Publishing House.

Simileanu, V. 2018a. "From frozen conflicts to hybrid warfare I." *GeoPolitica* Anul XVI (Nr. 73 (1)).

___. 2018b. "Hybrid warfare, conceptual approach." *Relații Internaționale. Plus* (Institute of International Relations of Moldova) (nr. 1): 32-43. https://ibn.idsi.md/sites/default/files/imag_file/32-43.pdf.

___. 2019. "The impact of hybrid threats on regional security." *GeoPolitica* Nr. 7.

Stancu, M.C. 2019. "Hybrid warfare and its forms of manifestation in the Ukraine crisis." *Gândirea Militară Românească* Nr. 2: 5-26. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/stancu.pdf.

Tzu, S. 2019. *The art of war.* Bucharest: Cartex Publishing House.

Wither, J.K. 2020. "Defining hybrid warfare." *per Concordiam: Journal of European Security and Defense Issues* (George C. Marshall European Center for Security Studies) 10 (1): 7–9. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf.

Wójtowicz, T. 2021. "Chinese concept of unrestricted warfare: Characteristic and contemporary use." *Humanities and Social Sciences.* https://doi.org/10.7862/RZ.2021.HSS.39.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Comprehensive Defence. Considerations Regarding the National Implementation of the Resistance Concept

Lieutenant Colonel Cezar-Vasile SOPON*

*Ministry of National Defence, Bucharest, Romania
e-mail: cvsopon@mapn.ro

Abstract

In the context of the deterioration of the security environment on NATO's eastern flank, many European states have intensified the development of additional defence mechanisms alongside traditional diplomatic and military instruments, aimed at deterring adversaries and countering both conventional and hybrid threats. One such mechanism involves integrating the whole of society into the national and allied defence effort. However, the adoption and implementation by Black Sea states of modern concepts associated with Comprehensive Defence, resilience, and resistance represent a complex process requiring substantial adaptation to national specificities, the nature of the threats, and lessons identified in ongoing or recent conflicts. This article examines the possibilities for implementing at the national level in Romania an Asymmetric Defence Component as an essential element of Comprehensive Defence.

Keywords:
Society; Comprehensive Defence; Asymmetric Component; Deterrence; Resilience; Resistance.

Article info
Received: 13 February 2026; Revised: 25 February 2026; Accepted: 16 March 2026; Available online: 8 April 2026

Citation: Sopon, C.V. 2026. "TComprehensive Defence. Considerations Regarding the National Implementation of the Resistance Concept." *Bulletin of "Carol I" National Defence University*, 15(1): 220-238. https://doi.org/10.53477/2284-9378-26-13

Dynamism, asymmetry, and unpredictability are frequently associated with the contemporary security environment, often correlated with the manifestation of hybrid threats and with the increasing role of non-state actors and civilian populations in the conduct of modern conflicts (Kilcullen, Counterinsurgency 2010, 34-36). Relevant examples can be observed in the development of territorial defence structures in the Baltic states, where the participation of civil society contributes to strengthening resilience and national defence capacity. At the same time, contemporary conflicts, such as the one in Ukraine, highlight the essential role of societal resilience and population mobilisation in supporting states' capacity to withstand external aggression (Mälksoo 2024, 12).

From a historical perspective, the involvement of society in matters of security and defence has often proved to be an important factor both in deterring hostile intentions and in ensuring an adequate response in situations of conflict. Over time, small organisations composed of members of society with limited military training and modest equipment have, by exploiting the advantages offered by knowledge of the environment and the support of the population, managed to create significant imbalances in the balance of forces and to affect the adversaries' morale (Kilcullen, Counterinsurgency 2010, 38-40; Szenes 2024, 5).

The motivation for selecting this topic lies in the need to deepen the study of possibilities for expanding national defence capabilities through the integration of the whole of society into the national defence effort, especially given that, in recent years, NATO has placed increasing emphasis on strengthening societal resilience, considered an essential element of collective defence and of states' capacity to cope with contemporary crises and conflicts (NATO 2024). This paper represents a structured analytical endeavour, based predominantly on inductive reasoning, through which existing theoretical models regarding Comprehensive Defence and resistance are analysed, and the possibilities for their adaptation at the national level are evaluated. While the first two chapters address, from a theoretical perspective, the characteristics of the main models and concepts associated with Comprehensive Defence and resistance, the third chapter examines how the previously detailed theoretical models may be adapted and implemented at the level of Romania.

Given the specificity of these instruments, associated with the field of security and defence, the specialised literature available in open sources is relatively limited and mainly includes information formulated at a high level of generality. In this context, the analysis carried out in this paper is based primarily on unclassified doctrinal documents and specialised studies relevant to the field of security and defence.

1. Comprehensive Defence

In recent literature, the resilience of a nation is analysed as a central element of national security, being associated both with the capacity of institutions to function

under crisis conditions and with the mobilisation of societal resources in support of defence (Szenes 2024, OECD 2024). One of the most frequently referenced concepts within NATO when addressing the active involvement of civil society in achieving national security objectives is *"Comprehensive Defence" (CD)*. The concept is grounded in Article 3 of the Treaty, which stipulates that, alongside the need for collective defence of the Alliance, it is equally important to maintain and develop the individual national defence capacity of each member state. At the level of certain European states, such as Sweden or Finland, the involvement of the whole of society in the national defence effort is conceptualised through *"Total Defence"* models, which entail the integration of civilian, economic, and military resources in support of national defence (Wither 2020, 63). These models are associated in recent literature with the development of a security culture at the societal level and with an increased degree of involvement of civilian actors in supporting national defence (Wrange 2024, 6).

In order to support member states in developing a national defence capability anchored in the realities of the current security environment, a series of non-binding documents has been elaborated at the Allied level, outlining the possibilities and modalities through which society may be integrated into the national defence effort. The most relevant documents in this regard are the *Resistance Operating Concept* – ROC (Fiala 2020) and the *Comprehensive Defence Handbook* – CDH (NATO Special Operations Headquarters 2020, 15).

From a theoretical perspective, the CD concept is defined as an *"official governmental strategy aimed at protecting national interests against potential threats through the involvement of the whole of society"* (NATO Special Operations Headquarters 2020, 15). Such an approach is designed to be effective both against threats generated by state actors and against those originating from non-state actors, natural phenomena, or major accidents. The levels/layers of CD are illustrated in Figure 1.

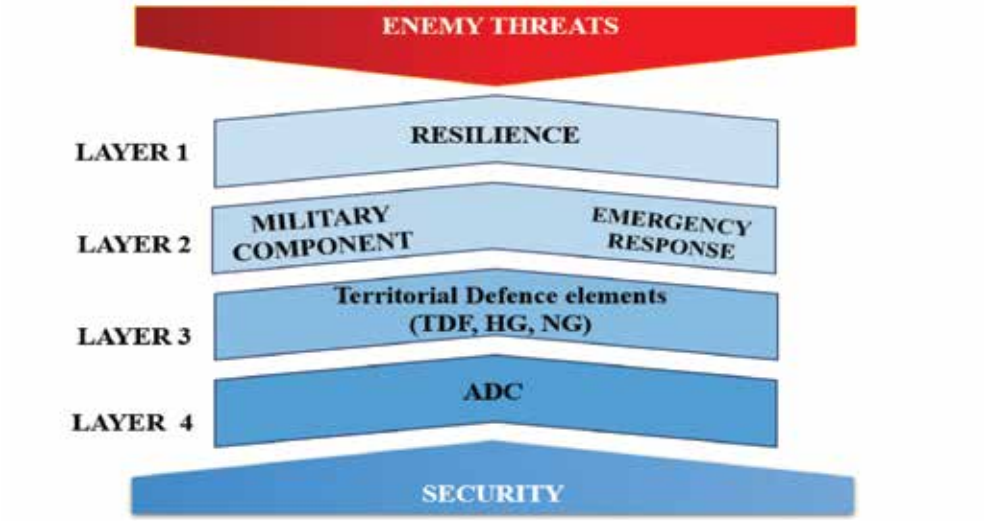

Figure 1 Illustration of the layers of CD

Source: rauthor's own elaboration based on NATO Special Operations Headquarters 2020, pp. 33–34

It can thus be observed that the second layer of CD represents the traditional response ensured through the state's specially designated structures: the armed forces (including reservists), structures of the Ministry of Internal Affairs (police, gendarmerie, emergency services, border police, etc.), intelligence services, specialised cyber defence structures, and others. Considering that the focus of the present paper is placed on the *Asymmetric Defence Component* (ADC), the second layer will be addressed only from the perspective of its links and implications for the ADC.

Resilience represents the cornerstone of Comprehensive Defence, ensuring its consistency, flexibility, and stability. It is considered an essential element of national security, representing the capacity of society to maintain the functioning of institutions and to support the defence effort in situations of crisis or conflict (Szenes 2024, 5). The concept is defined as "the capacity of societies to resist, adapt and recover from major shocks, including security crises or armed conflicts" (OECD 2024). In international specialised literature, several concepts may be associated with the third layer, the most widespread being *Home Guard* (HG), *National Guard* (NG), and *Territorial Defence Forces* (TDF). Although similar, these concepts are not identical, as each nation adopts different approaches regarding the characteristics, organisation, and responsibilities of such structures. In general, the concepts listed above refer to groups of volunteers or reservists organised and coordinated by state institutions, which contribute to various aspects of national or Allied security (NATO Special Operations Headquarters 2020, 17).

In Romania, such structures included the *"Patriotic Defence Guards"*, which operated for a short period beginning in September 1944, and the *"Patriotic Guards"*, established in 1968 (Romanian State Council 1968) in response to the occupation of the Czechoslovak Socialist Republic by the Soviet Union, and which remained operational until the Romanian Revolution of 1989.

In order to avoid associating HG, TDF or NG type structures with Romania's current efforts to diversify recruitment and staffing modalities and, at the same time, to avoid using the historically established Romanian equivalent of these concepts – *"Patriotic Guards"* – which could generate confusion due to its historical connotations, this paper employs the generic term "*Territorial Defence Elements*" (TDE). By TDE, we refer to territorial defence structures within the HG, TDF, and NG spectrum, organised in a manner similar to conventional forces, which have the role of increasing the national capacity to provide a response to various situations. Regardless of the territorial defence model adopted, such structures can fulfil a variety of responsibilities, including support to civilian authorities, protection of infrastructure and population, participation in the management of emergencies, and support for military operations (NATO Special Operations Headquarters 2020, 38).

2. The Asymmetric Defence Component

In defining and properly understanding the ADC, one may start from the broader concept of resistance, with which it is most often equated.

The word *"resistance"* has multiple meanings and may sometimes generate confusion. Used in a generic sense, *"resistance"* refers to the ability of a system to withstand a certain factor. When addressing a security or defence context, however, the term "resistance" represents the *"effort of the whole of society, organised and led by a legitimate government (understood as legitimate political leadership formed by state authorities), potentially in exile, relocated, or operating 'from the shadows', encompassing both violent and non-violent activities aimed at restoring independence or autonomy within national territory partially or totally occupied by an occupying force"* (Fiala 2020, 5). Another term within this conceptual sphere is *"national resistance"*, which differs from *"resistance"* and is defined as a capability based on pre-planned, pre-conflict efforts to establish the legal framework, develop plans and employ resistance in the event of aggression or occupation (Fiala 2020, xv-xvi). In certain contexts, the term *"resistance"* may refer both to the organised effort of society to oppose an occupying force and to the individuals or groups that participate in these actions (Fiala 2020, 5).

Another concept within the sphere of the term *"resistance"* is the "*resistance movement"*, which in specialised literature is generally associated with the opposition of organised groups against a legitimate political leadership, most often supported by state entities lacking legitimacy over the respective territories, with the general objective of changing the legitimate political leadership. The term *"resistance movement"* is more commonly associated with the concept of *"unconventional warfare"*, as defined in American doctrine (U.S. Department of Defense 2024, II-9).

In order to avoid confusion and to emphasise the strictly defensive character of CD, the term ADC is introduced, defined as that component of CD which provides the nation with the ability to conduct, under the leadership of state institutions, whole-of-society resistance against an occupying force, with the aim of maintaining/restoring independence and territorial sovereignty (NATO Special Operations Headquarters 2020, 43). ADC represents the fourth layer within CD, yet it plays a particularly important role in achieving the first layer, resilience.

In recent literature, the organisation of resistance is analysed as a complex system that includes clandestine structures, logistical support elements, and armed components capable of conducting actions against an occupying force (Barno and Bensahel 2023). ADC, similarly to the resistance movement described in the specialised literature on unconventional warfare, operates in territory under enemy control and uses structures and networks that can operate clandestinely in order to support resistance elements. Its structure (Figure 2) comprises four interconnected components (NATO Special Operations Headquarters 2020):

- *the Underground (UG)* – responsible for ensuring the organisation's leadership; in the specialised literature, this component may also be referred to as "clandestine networks", being responsible for coordinating activities and maintaining communications between the different components of the resistance, thus ensuring the coherence of actions carried out against occupying forces (Paul, Helmus and Glenn 2023, 22).
- *the Adapted Force (AdF)* – the operational response element;
- *the Auxiliary (AUX)* – provides support to all ADC elements. This component is also referred to in the specialised literature as "support networks" and has an essential role in providing logistical and intelligence support (Paul, Helmus and Glenn 2023, 25).
- *the public component* – representing the political dimension of ADC.

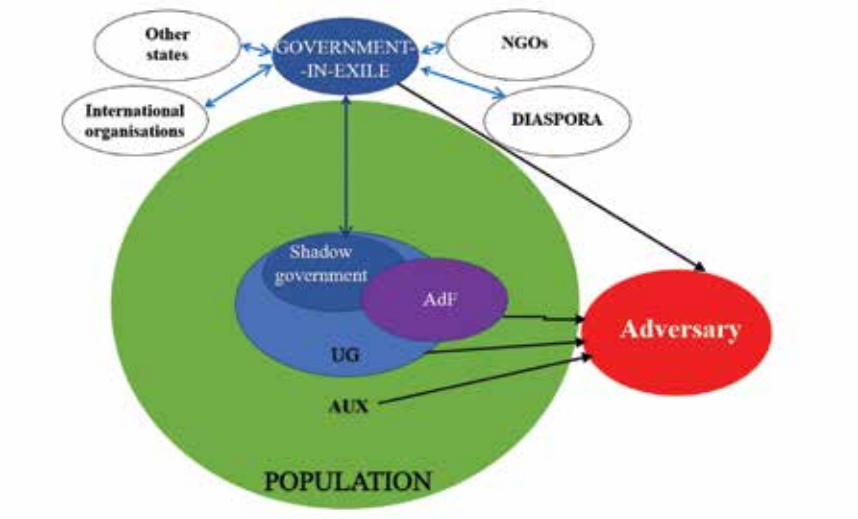

Figure 2 ADC structure
Source: adapted from NATO Special Operations Headquarters 2020, p. 43

As a methodology for developing ADC capabilities, the joint functions may be employed, as they support resource prioritisation and the integration of the organisation's constituent elements. The responsibilities of ADC in relation to the joint functions are graphically illustrated in Figure 3.

Figure 3 Functions of the Resistance Elements
Source: adapted from US SOCEUR 2022, p. 2

The description of the elements may be summarised as follows:

- *command and control (C2)* – includes the command and control architecture (regional and zonal commands, subordinate command elements), inter-institutional coordination, and the development of information management capabilities;
- *information operations* – ensure the achievement of non-lethal effects.
- *protection* – encompasses the capabilities that ensure the security of actions, communications, personnel, and the population;
- *sustainment* – in addition to traditional logistic support, includes personnel-related aspects, medical support, and financial support;
- *intelligence* – ensures understanding of the environment and is essential for the conduct of resistance activities. It includes counterintelligence, collection, analysis, and dissemination capabilities;
- *fire support* – enables the creation of lethal and non-lethal effects against targets. It requires both an internal target management process and one at the joint level, particularly for targets requiring the engagement of external capabilities;
- *movement and manoeuvre* – ensures freedom of movement within the area of responsibility and the positional advantage necessary for engaging enemy elements, especially by AdF.

The four components of ADC are in a dynamic relationship, influenced by both internal and external factors. UG is primarily responsible for leading and coordinating resistance activities, while AdF represents the operational element that conducts actions against the occupying force (NATO Special Operations Headquarters 2020, 46).

In Romania, the Government "*ensures the implementation of the country's domestic and foreign policy and exercises the general leadership of public administration*" (Romanian Government 2026). In the context of CD, the *term "government"* essentially refers to "legitimate political leadership", not necessarily strictly limited to the executive branch, and encompasses the legitimate state authorities and institutions exercising decision-making, regulatory, representative, or executive roles.

In the event of total or partial occupation of national territory by the enemy, should the primary location be compromised, political leadership may be ensured either through the relocation of central authorities to a non-occupied area, through a *"government in exile"*, and/or through a *"shadow government"* operating clandestinely within the occupied territory (Fiala 2020, 5-6).

In the most likely situation, in which legitimate political leadership functions from outside the occupied area (either from unoccupied national territory or from exile), the term "shadow government" designates only the territorial element deployed within the occupied area, operating clandestinely and coordinating resistance

activities. At the same time, it functions within ADC, receives direction from the institutions ensuring proper governance, and constitutes the core leadership element and, simultaneously, the expression of the state's continued existence within the occupied territory.

On the other hand, the underground element represents the resistance component with the greatest number and variety of responsibilities, including ensuring ADC leadership and executing actions in areas inaccessible to AdF.
UG exists and operates clandestinely, relying on leaders who, through flexibility and vision, are capable of ensuring the timely adjustment of actions, organisation, and C2. UG command is centralised, while execution is predominantly decentralised, thus ensuring both effective coordination of operational elements and operational security. It is particularly important that at least the essential elements of UG be organised and functional already in peacetime.

The key responsibilities of UG (Fiala 2020, 20) include:

- *recruitment of members* – this task is essential and involves identifying, vetting, contacting, and integrating the personnel required for the diverse responsibilities of resistance;
- *intelligence support* – this function is considered directly responsible for the success or failure of resistance and encompasses planning/direction, collection, analysis, and dissemination of three categories of information: military information, information necessary for the execution of sabotage, and political information;
- *financing* – the underground element is responsible for securing and managing financial resources for the entire resistance. Particularly important are financial resources provided by legitimate authorities (for example, those in exile), those granted by non-state actors, and those received from other states;
- *logistic support* – this function is planned and supervised by UG, while execution belongs to AUX. It encompasses all activities related to procurement, storage, and distribution of goods and supplies, as well as maintenance, medical, and transport services. Another measure that may be considered in preparing national territory for defence is the establishment in peacetime of secret "cache" type depots, which may be used by the resistance in the event of occupation;
- training of ADC members during occupation – UG is primarily responsible for the training of all ADC members;
- *communications* – vital for ensuring the success of resistance actions and for their effective integration into the CD effort. The underground element is responsible for both ensuring the internal information flow within ADC and for communication between ADC and external actors;
- *security* – represents an essential element in ensuring the functionality and survival of the underground element and, implicitly, of ADC. It is primarily

the responsibility of UG, although AUX also contributes significantly (for example, through early warning). In general, UG must be integrated within civil society, following the principle: "the more you succeed in behaving like an ordinary citizen, the less suspicious you will become" (US Army Institute for Military Assistance 1978, 69).

In addition to the key responsibilities outlined above, UG is the principal ADC element responsible for planning and executing information operations within occupied territory and for carrying out acts of sabotage and subversion.

AdF represents the ADC element responsible for conducting military actions of a kinetic and/or lethal nature, in accordance with the direction received from UG. The term "Adapted Force" is preferred over the term "guerrilla", frequently used in specialised literature, as the latter does not necessarily imply that such structures are organised and controlled by legitimate leadership, as is the case with ADC. AdF represents a combination of traditional military structures and elements of society and may include: military personnel and units, reservists, territorial defence structures, and volunteers. As a rule, AdF is smaller in size than the other ADC elements.

Unlike traditional armed forces, AdF is organised into small operational elements, primarily armed with light infantry weapons. Among the most frequently employed techniques are raids, ambushes, and sabotage. The primary purpose of AdF actions is to deny the enemy freedom of movement and to degrade its combat capability (Fiala 2020, 27).

AdF structures are generally organised in cells (ranging from a few members to several dozen), geographically distributed (for example, in the area of a rural locality, one or more cells may operate). AdF generally has a limited vertical development, with cells subordinated directly to regional or zonal commands or to UG leadership cells (Fiala 2020, 26-27).

The recruitment of AdF should already be initiated in peacetime, at least at the leadership level. Given their prior military training and vetting, members of TDE constitute an especially valuable recruitment base. For this reason, it may be more advantageous for a certain number of members to remain within occupied territory and to be integrated into AdF.

AUX does not constitute an organisation in itself, does not possess a formal structure, and has no independent leadership. It represents that part of society which performs tasks in support of resistance, at the request and under the coordination of UG or AdF. AUX is composed of members of society who participate in resistance activities only occasionally and on a task-specific basis, carrying out highly specialised tasks. Members of the auxiliary element are aware of resistance activities only to the extent strictly necessary for the fulfilment of their assigned duties. The principal activities in which AUX is involved include: procurement and distribution of goods and supplies; manufacturing of specialised materials; provision of security through early warning; intelligence collection; support to recruitment activities; provision

of communications; distribution of media materials; administration of resistance facilities; logistic activities and transport services (Fiala 2020, 27).

The public component of ADC represents the extension, image, and public face of legitimate political leadership within the occupied territory. It may consist of a single public personality or of a more complex structure. Depending on the situation or the degree of tolerance shown by the enemy, the public component may negotiate directly with it, may take the form of an opposition political party, or may operate clandestinely.

A useful model in the creation and employment of ADC may be the National Resistance Model (NRM), which comprises six phases (US SOCEUR 2022, 22):

- *preparation* – includes activities such as determining the feasibility and necessity of resistance, establishing the legal framework, defining responsibilities and inter-institutional relationships, and preparing the population through specific narratives. Particularly important in this phase is the establishment of the levers and instruments necessary for recruitment, training, and activation of members;
- *capability development* – in this phase, the necessary infrastructure, networks, and ADC capabilities are developed. Initial efforts focus on developing those elements that ensure the survival, control, and subsequent development of resistance. At the end of this phase, ADC elements are synchronised and capable of conducting violent and non-violent actions against an occupying force or aggressor;
- *engagement* – involves activating zonal commands and engaging the enemy, gradually increasing pressure and regaining control over occupied areas;
- *consolidation* – exploits previous success and, together with conventional forces, creates the conditions for repelling the aggressor and liberating national territory;
- *liberation* – through the success of previous phases, the majority of society is mobilised in support of ADC through non-violent activities. At this stage, AdF reconfigures its operational posture by concentrating forces into larger elements and conducts large-scale actions integrated into the liberation operation (executed, for example, with the support of Allied military structures). Subsequently, a link-up with conventional forces takes place;
- *transition* – involves the transfer of authority to the responsible structures within the national defence, security and public order system and the return to the pre-occupation state.

In conclusion, specialised literature on national resistance analyses existing models primarily through the lens of American unconventional warfare doctrine. Although American doctrine details the components and internal processes of resistance, it focuses predominantly on supporting elements of society in a foreign state in their effort to replace legitimate political leadership. By contrast, European models aim

at deterring the aggressor and ensuring state survival. These differences require the adaptation of resistance priorities, infrastructure, and operating procedures so that it may be effectively integrated into the national defence effort.

3. Applied Analysis Regarding the Organisation of the Asymmetric Defence Component within Romania's National Territory

This chapter has a predominantly analytical character and includes a conceptual exploration of how ADC could be implemented at the national level, in accordance with the theoretical foundations presented in the previous chapters, as well as with Romania's particularities and national specificities. The analysis uses a simplified scenario, constructed exclusively on the basis of information available in open sources, with an illustrative role in assessing the applicability of the theoretical model, without representing elements of actual operational plans. Within this analytical endeavour, the aim is to formulate an answer to two main questions:
- *"How can ADC be organised optimally and efficiently at the level of Romania?"*
- *"How can the recruitment and training of ADC members be conducted in peacetime?"*

From a methodological perspective, the paper employs a qualitative approach, the main instruments and techniques being the vignette, conceptual modelling, experimentation, and observation. The vignette was selected as it allows for the construction of a controlled analytical framework and the establishment of specific parameters and details, facilitating the analysis of particular situations without requiring the development of complex scenarios (NATO Science and Technology Organisation 2015, 2-10). Within this analytical endeavour, the vignette is used to assess how the previously discussed theoretical concepts can be adapted at the national level.

Conceptual modelling is employed to represent the relationships between the main components of the resistance system and to identify possible organisational structures. Observation enables the interpretation of the results obtained in relation to the specialised literature and to existing examples in states that use similar defence models. The experiment has an exploratory character and consists of the conceptual testing of the proposed model by applying it within the analysed scenario, with the aim of evaluating the functioning of the relationships between the components of the resistance system.

The general analytical framework is defined by the following elements:

- *The security context* is defined by an analytical scenario inspired by recent developments in the security environment of the Black Sea region
- *The target area* for organising resistance is the Dobrogea region.
- *The time horizon* is three years, during which resistance structures must become capable of self-management, contributing to the repelling of

aggression or supporting the liberation of occupied territory.

- *Concerning the civilian population*, it is assumed to be characterised by a moderate level of attachment to national values/patriotism and a moderate willingness to participate in the defence of the national territory, the population being rather inclined to leave the conflict area. At the level of the target area, it is estimated that there are approximately 100,000 men who have completed military service, relatively evenly distributed across administrative-territorial units.

- *The current national legislative framework* is not considered a limiting factor, as the political decision-maker demonstrates openness to adapting it according to necessity.

The main elements resulting from the operational environment analysis (PMESII-PT) are as follows:

• ***P**olitical:* The existence of a large number of administrative-territorial units of the commune and town type allows for a balanced dispersion of ADC elements. The size of the municipality of Constanța, the existence of a developed administrative apparatus, and numerous logistic facilities recommend this urban concentration as the primary option for the functioning of a regional resistance command.

• ***M**ilitary* (semi-fictional): Within the target area, military structures belonging to all service branches are deployed, including a mechanised infantry brigade, a marine infantry regiment, naval fleet forces, elements of the river flotilla, and two air bases. In addition, three TDE battalions staffed with reservists and volunteers are deployed in the area, whose personnel have undergone the necessary training to master basic techniques, tactics, and procedures.

• ***E**conomic:* The diversified regional economy may provide the resources necessary for sustaining resistance. At the same time, considering that during a conflict or occupation the service sector is particularly affected, and that a significant proportion of the active population is employed in this sector, a considerable level of popular support for resistance may be anticipated.

• ***S**ocial:* The ethnic configuration represents a relevant element, with the Romanian ethnic population exceeding 90%, the other significant ethnic groups being Turkish and Tatar. This proportion is similar with regard to the Orthodox religion. The distribution by gender and age categories is relatively balanced. The level of education is higher in urban areas, lower in the central and north-eastern areas, and medium in the north and west. This configuration makes it difficult to justify a potential occupation and facilitates the clandestine functioning of resistance.

• ***I**nformation:* In the event of degradation or disruption of mobile communication networks and internet access, efforts to inform the population will need to be redirected towards printed materials and radio broadcasts transmitted from outside the target area. In order to maintain ADC's internal and external information flow, alternative communication solutions are required.

- ***Infrastructure:*** Road, maritime, and river infrastructure supports the functioning of resistance by ensuring the mobility of personnel and goods within the area, but limits personnel and material flows from and to the outside. Solutions may be identified through the development of AUX capabilities in localities along the Danube floodplains and through the use of small craft.
- ***Physical environment***: Dobrogea represents a distinct geographical area, bounded by water on three sides. The terrain consists predominantly of hills and plateaus (100–300 m) in the central and southern areas, with floodplains along the Danube, delta areas in the north-east, and lagoon coastline in the east. The hydrographic network includes the Danube River with its branches and delta, lagoon lakes, and the Danube–Black Sea Canal. The accessible terrain has enabled the development of good road infrastructure and a relatively uniform distribution of settlements (over 75% of the surface area), with minimum density in the north-east and maximum density in the south-east.
- ***Time:*** The time factor represents a significant constraint, requiring the priority creation and organisation of essential ADC elements, with their further development to be carried out progressively upon the emergence of a crisis or during occupation.

With regard to the organisation and development of ADC, these will be conducted during the first two phases of NRM, as outlined in the theoretical framework presented in Chapter 2. The first phase is predominantly the responsibility of the political factor and will be addressed at a general level.

a) Phase I–Preparation – approximately 12 months. The duration and activities of this phase result from adapting the previously presented NRM model to the specifics of the analysed scenario. The main activities are detailed in Table 1.

TABLE no. 1. Main Activities Associated with the Preparation Phase

Nr. crt.	Task	Actions	End state
1.	Determining whether the establishment of a resistance structure is feasible	Feasibility study, identification of implications, and calculation of required resources	Confirmation of the assumption that the establishment of ADC is necessary, appropriate, and achievable
2.	Designation of responsible structures	Political and inter-institutional debates and negotiations	MoND designated as the responsible structure; establishment of specialised structures; allocation of responsibilities
3.	Creation of the legal framework	Amendment of existing legislation and regulations	The legal framework enables the creation and functioning of resistance
4.	Preparation of the population	Development and dissemination of narratives, public information materials, etc.	The population understands and agrees with involvement in the national defence effort

Once the requirements, responsible structures, and legal framework have been established, and public support has been secured, the actual development of ADC may begin.

b) Phase II – Capability Development – 24 months;

The main structures and C2 relationships of ADC are composed of the following elements:

- ***UG*** – comprising Regional Resistance Commands (RRC), which also integrate elements of the "shadow government", Zonal Resistance Commands (ZRC), local-level leadership cells, and specialised cells;
- ***AUX*** – composed of AUX cells providing support across various domains to all ADC elements;
- ***AdF*** – the element specialised in violent actions, organised into cells;
- ***the public component*** – representing the element that ensures the public representation of resistance within society and in relation to the enemy.

Extrapolating to the national level, the conclusions of the previously conducted PMESII-PT analysis, it is considered appropriate to organise resistance by regions, each region generally comprising between two and five county-level administrative-territorial units and being led by an RRC, subordinating several ZRCs. Each RRC is capable of fulfilling the functions specific to a "shadow government" or, as appropriate, integrating and ensuring the functioning of its elements, depending on the evolution of the operational situation.

With reference to the study's target area, the exercise of command and control will be conducted through RRC Dobrogea, with its primary location in the municipality of Constanța. Based on the analysis of geographical factors, the distribution of localities, and the C2 requirements of the resistance, Dobrogea was divided into ten distinct areas (Figure 4).

Figure 4 Areas of Responsibility of the ZRCs within RRC Dobrogea

Source: author's own elaboration based on the analysis of geographical and administrative factors of the Dobrogea region, using exclusively information from open sources.

Each of the ten ZRCs is capable, through the efficient use of available forces and resources, of accomplishing the tasks assigned by RRC Dobrogea. Figure 5 provides a generic graphical representation of the organisation and C2 relationships of the resistance. At the regional level, the RRC structures, the "shadow government", and the public component exist in a relationship of interdependence, ensuring the leadership functions of the entire ADC. They coordinate liaison with state and non-state actors, maintain contact with national authorities operating outside the occupied area, and conduct strategic communication and public representation activities.

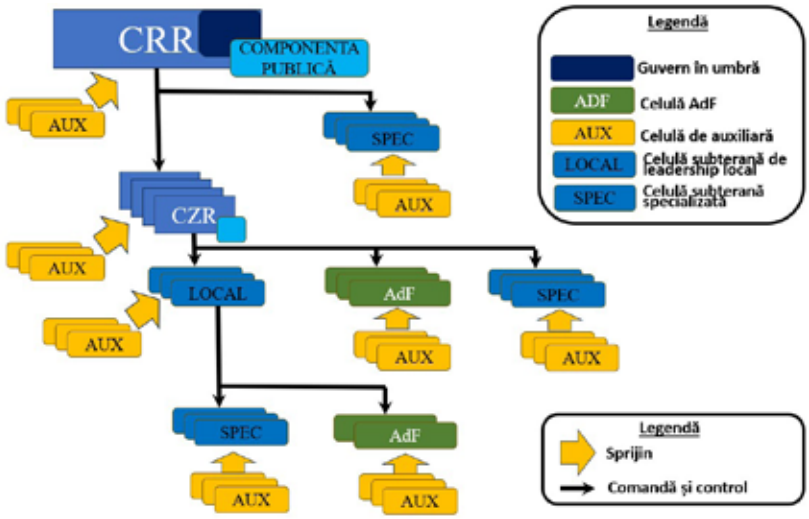

Figure 5 Generic Structure of ADC and C2 Relationships
Source: representation developed by the author based on the specialised literature (Fiala 2020; NATO Special Operations Headquarters 2020)

Analysing the average size of rural localities, of approximately 3,000 inhabitants, as well as their distribution within the target area, it is estimated that within each locality, between one and three small-sized cells may function optimally, each comprising several dozen members.

The development of ADC capabilities, both in peacetime and during periods of crisis, will be conducted under the coordination of the Department for Asymmetric Defence (DAD). This represents an inter-institutional structure subordinated to the Ministry of National Defence, specifically created for the development of the infrastructure necessary for ADC functioning, the integration of its activity into the national defence effort, and the coordination of recruitment, training, and equipping processes for its members. At the territorial level, within each region under the responsibility of RRC, DAD will subordinate a Regional Directorate for Asymmetric Defence (RDAD). Within the target area, ADC development is coordinated by RDAD Dobrogea, headquartered in the municipality of Constanța. DAD and RDAD do not exercise direct command over the resistance under occupation conditions. Their responsibility is confined to the development of capabilities, infrastructure,

and preparatory mechanisms required for resistance to function effectively during a crisis and potential occupation.
In order to conduct a realistic analysis, extrapolating publicly available data regarding the mobility of the Ukrainian population in areas occupied by Russia in the current conflict, we assume that in the event of aggression followed by occupation, through evacuation or relocation, the population of the Dobrogea region would decrease by approximately 60%, meaning that around 400,000 inhabitants would remain within the target area, distributed across approximately 120 localities. The most affected areas would be the urbanised zones in the south-east of the region.

The objective is that, during the consolidation phase of the NRM, under occupation conditions, in order to maintain an appropriate balance between organisational needs and the normal functioning of societal activities, resistance should comprise approximately 5% of the remaining population. The 5% estimate represents a balanced approximation within the limited range of active participation identified in classical insurgency and resistance literature, where only a small fraction of the population engages directly in operations, while the majority provides passive support or remains neutral (Kilcullen, Counterinsurgency 2010, 35). This implies that ADC infrastructure would need to sustain up to 20,000 members. The distribution by elements would be as follows:

- 20% within UG – 4,000 members;
- 15% within AdF – 3,000 members;
- 65% within AUX – 13,000 members.

Given the unpredictable nature of the situation, the application of a safety margin of at least 30% is recommended. At the same time, the figures mentioned represent the maximum potential size of the resistance, without implying the recruitment or simultaneous activation of all members. In peacetime, emphasis will be placed on the recruitment of leaders, specialists, and key personnel for the development, training, refinement, and validation of resistance processes and network functionality.

Correlating ROC recommendations with the previous analysis, the selection base is outlined as follows:

- ***UG:*** reservists, TDE members, informal leaders. The majority of these must be identified, vetted, and confirmed (establishing contact and confirming their intention to support resistance) already in peacetime. Some of them will be involved in organising and developing infrastructure, as well as in training and recruiting members.
- ***UX***: any citizen capable of supporting resistance. As the tasks of this component are simple and specific, members do not require a complex vetting or training process. Most of them may be recruited during a crisis or even during an occupation, depending on necessity.
- ***AdF:*** citizens with military training or who express willingness to undergo

training. TDE represents an essential instrument for identifying, vetting, and training AdF members. The activation of AdF cells and joint training, for security reasons, is recommended to take place at the earliest, during a crisis. Nevertheless, key personnel should be identified, vetted, confirmed, and trained, as far as possible, in peacetime.

The recruitment and training process of AdF members, both in peacetime and during crisis, is complex and challenging, particularly due to the need to ensure operational security. Training must be conducted in locations and conditions different from those in which members will operate, and the majority of members should not know precise details regarding their place and role within the network. For example, a reservist trained to occupy a position within an infantry battalion may be requested to remain within territory estimated to be occupied in order to fulfil tasks that will be communicated at a later stage.

Conclusions

Although inspired by American specialised literature on unconventional warfare, ROC and CDH may constitute the foundation for the development of an effective Comprehensive Defence. Alongside the national development and adaptation of these theoretical models, it is necessary to establish a solid, assumed, and dynamic normative framework.

In response to the question *"How can ADC be organised optimally and efficiently at the level of Romania?",* based on the analysis of environmental factors, an organisational model applied to the Dobrogea area was developed, which may be extrapolated to the entire national territory or even to other states within the Black Sea region. The implementation of this model requires the creation of a legal framework supporting the functioning of specialised structures, at both central and regional levels, responsible for coordinating the entire resistance organisation process. The organisation of ADC across multiple C2 levels entails: regional commands covering generally two to five counties and subordinating six to twelve zonal commands, usually located in urban areas and responsible for adjacent areas. For the sake of efficiency, ADC must necessarily be organised in peacetime, particularly with regard to network infrastructure, processes, and staffing with key members.

The response to the question *"How can the recruitment and training of ADC members be conducted in peacetime?"* highlights the need to establish TDE-type structures, which would allow the establishment of contact, vetting, and training of potential resistance members within an appropriate framework. Such an approach would considerably expand the selection base for ADC, support the mitigation of the continuous decline in the number of citizens with military or security training, and contribute to the development of both individual and national resilience.

In light of the above analysis and conclusions, in the event of an intention to organise resistance at the national level, the following proposals may be formulated:

- A detailed study should be conducted regarding public perception of organising resistance at the national level. In the case of an unsatisfactory result, it is critical to successfully conduct extensive campaigns promoting national values and developing security culture, responsibility, and patriotism.
- A significant number of TDE structures should be established at the territorial level, both to compensate for the effects of the reduction or ageing of reservists and as the principal mechanism for recruiting and training resistance members.
- Based on thorough analysis and testing, dedicated structures should be established for the organisation, development, and command of resistance, both at central and territorial levels, integrating and coordinating the efforts of institutions with responsibilities in defence, public order, and national security.

References

Barno, David, and Nora Bensahel. 2023. "The Future of Resistance Warfare." *War on the Rocks.* Accesat 15 martie, 2026. https://warontherocks.com/2023/04/the-future-of-resistance-warfare/.

Fiala, O. 2020. *Resistance Operating Concept.* MacDill Air Force Base, FL: The JSOU Press.

Kilcullen, D. 2010. *Counterinsurgency.* Oxford: Oxford University Press.

Mälksoo, Maria. 2024. "Societal Defence and the War in Ukraine." *Journal of Strategic Studies* 1-18.

NATO. 2024. *Resilience and Civil Preparedness: Allied Approaches to Societal Security.* Brussels: NATO.

NATO Science and Technology Organisation. 2015. *TR-MSG-086-Part-II Guideline on Scenario Development for (Distributed) Simulation Environments.*

NATO Special Operations Headquarters. 2020. *Comprehensive Defence Handbook Vol.1, Ed. A, Vers 1.* Bruxelles.

OECD. 2024. „Building Resilient Societies: Policy Perspectives." Paris: OECD Publishing.

Paul, Christopher, Todd C. Helmus, and Russell W. Glenn. 2023. *Resistance and Irregular Warfare in Modern Conflicts.* Santa Monica, CA: RAND Corporation.

___. 2023. *Resistance and Irregular Warfare in Modern Conflicts.* Santa Monica, CA: RAND Corporation.

Romanian Government. 2026. *Pagina oficială a Guvernului României.* https://www.gov.ro/ro/guvernul.

Romanian State Council. 1968. *Decret nr. 765 din 4 septembrie 1968 privind constituirea, organizarea și funcționarea gărzilor patriotice.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/46433.

Szenes, Zoltán. 2024. „Societal Resilience and National Defence in the 21st Century." *Defence Studies* 24 (1): 1-18.

U.S. Department of Defense. 2024. „Joint Publication 3-05: Special Operations." U.S. Department of Defense, Washington, DC.

US Army Institute for Military Assistance. 1978. *ST 31-202: The Underground.* Fort Bragg, NC, SUA.

US SOCEUR. 2022. *Resistance Operational Guidance.* Stuttgart.

Wither, James K. 2020. "Back to the Future? Nordic Total Defence Concepts." *Defense & Security Analysis* 36 (1): 61-81.

Wrange, Joakim. 2024. "Resilience through Total Defence: Towards a Shared Security Culture in the Nordic-Baltic Region." *European Journal of International Security* 9 (1): 1-20.

CONFLICT OF INTEREST STATEMENT

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

DATA AVAILABILITY STATEMENT

This article does not rely on primary datasets requiring public archiving.

STATEMENT ON THE USE OF AI

The author declares that artificial intelligence tools were used exclusively for linguistic refinement and translation support, without involvement in the development of the scientific content of the paper. The author retains full responsibility for the content of the article.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Credibility of Public Diplomacy Narratives in the Age of Fake News and Growing Mistrust Among International Political Actors

Assoc. Prof. Ecaterina HLIHOR, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: hlihor.ecaterina@myunap.net

Abstract

The possibility of a widespread conflict between actors possessing nuclear weapons and ultra-sophisticated military technologies is increasingly mentioned in academic analyses and debates, causing concern among the international public. Democracy as a form of government in peaceful times can undergo fundamental changes in situations of conflict. The political leaders of the major powers can use democracy and diplomacy to reduce or prevent war, but when violence breaks out between two states, both sides use democracy to make people sympathise with their objectives and tactics and to damage the reputation and image of the other side. Under these conditions, psychological warfare and information warfare gain more importance and applicability than public diplomacy activities. And yet, in this conflictual communicative environment, public diplomacy does not disappear from the international public agenda. The stakes are 'whose public diplomacy narrative wins' rather than 'whose army wins,' because international politics and communication have entered a competition of credibility. The answer to this question is complicated because the communication environment has changed in the digital age, with wars involving multiple forms of violence. In this type of international conflict, there are several communication actors who play the role of narrators with different objectives, and the credibility of public diplomacy messages and narratives is affected by the phenomenon of fake news and post-truth.

Keywords:

Public Diplomacy Narratives; Global Wars; Credibility of Public Diplomacy; Propaganda; Cognitive Warfare.

Article info

Received: 12 February 2026; Revised: 20 February 2026; Accepted: 16 March 2026; Available online: 8 April 2026

Citation: Hlihor, E. 2026. "The Credibility of Public Diplomacy Narratives in the Age of Fake News and Growing Mistrust Among International Political Actors." *Bulletin of "Carol I" National Defence University*, 15(1): 239-251. https://doi.org/10.53477/2284-9378-26-14

'Winning the hearts and minds' of an audience in another society is an expression commonly used in the context of public diplomacy activities and is the main goal of any public diplomacy activity. The phrase 'win hearts and minds' was first used by US President Lyndon B. Johnson while preparing the public opinion for the intervention in Vietnam: 'So we must be prepared to fight in Vietnam' (...) 'but the final victory will depend on the hearts and minds of the people who live there' (Hess 2015, 112). In fact, the president's speech was a rhetorical device for what military specialists (Memorandum 1968) at the time and analysts today have defined as 'the other war' in Vietnam (Hemingway 1994; Peterson 1989). It was also a signal to certain media organizations and the American elite to use cultural and artistic strategies and means to gain the support of the Vietnamese people against the communist insurgency. Today, the expression is still used to describe efforts to create a favourable image of a country or group in the eyes of foreign audiences, with the aim of building trust, understanding, and cooperation. A wide range of activities is used to achieve this goal, including cultural exchanges, educational programs, media involvement, and public discourse by cultural and academic elites. These activities aim to promote the values, interests, and policies of a country or group and create a positive image in the minds of foreign audiences. Successful public diplomacy campaigns have a significant impact on a country's reputation and influence in the world, as well as on its ability to achieve its foreign policy goals. By interacting with foreign audiences and building relationships based on trust and mutual understanding, public diplomacy can contribute to a safer, more peaceful world.

An essential element in achieving the objectives pursued in public diplomacy is the credibility of the message. Credibility is the initial basis for motivating a target audience to decide to listen to someone's message. In a geopolitical and geostrategic context dominated by security and relationships of esteem and cooperation between different actors on the international stage, achieving real credibility with the target audience does not seem so difficult. It is not as easy to gain credibility in public diplomacy when uncertainty and the psychosis of global conflict dominate international politics, as has been the case in recent years. In such a world, psychological warfare and information warfare seem to gain more importance and applicability than public diplomacy activities. Deep-fake and fake-news phenomena strongly erode people's trust in messages circulating through various channels in international communication, including those specific to public diplomacy.

From this perspective, we aim in this study to analyse the current environment and communicative changes in public diplomacy in an era of uncertainty and globalization of conflicts. Two essential research questions for this analysis arise from the aforementioned objective: 1. What has changed in the communication environment of public diplomacy today? 2. What are the winning narratives of public diplomacy in this period? To answer these two questions, this study examines the transformations in the phenomenon of war and in the communication environment

that are taking place in today's modern world. The actors who communicate today in the new environment, the credibility of the narratives and messages conveyed to different target audiences, and the functioning of soft power as a narrative/exposure of the country's values through public diplomacy will be analysed. The paper will first explore the transformations and changes that have taken place in conflicts in recent years in different regions of the world, and then the significance of narratives and their importance in public diplomacy activities, and their connection to soft power used by actors involved in conflicts of lesser or greater magnitude. Given that today's world is characterized by interconnected societies, social networks, and multiple communication actors, the environment of public diplomacy is also changing. In addition, trust in information and narratives disseminated online is declining. This requires an explanation of the concepts of post-truth and cognitive warfare (fifth-generation warfare), which are linked to fake news and manipulation through the use of words as weapons (Saliu 2023, 209-224).

Change and continuity in the nature and character of war. Is public diplomacy becoming a player on the battlefield?

Observation and research of war throughout history have shaped and established multiple representations of this phenomenon, which have followed one another under the pressure of both objective and subjective factors (Hlihor and Băncilă 2024, 32-60). Throughout history, its essence as a social and political phenomenon has remained constant. Violence, bloodshed, imposing one's will on the defeated, cohesion in battle, camaraderie within units, the concept of honour—these remain unchanged. However, the character of war—the way wars are fought in terms of the strategic environment, technologies, weapon systems, creativity in combat, and leadership—is changing rapidly. The conflicts of recent years, particularly those in Ukraine and Gaza, have highlighted the first signs of a transition to a completely new paradigm: the era of digital warfare, with a multidimensional battlefield in which, alongside the physical dimension, cyberspace and the information environment are becoming increasingly important. Classic combatants, who use instruments of physical destruction against their adversaries, are assisted by specialists trained to use the weapons of words and images. This category of combatants also includes professionals in public diplomacy (Sukhorolskyi and Sukhorolska 2024, 272; Hlihor 2023, 20).

Geopolitical and geostrategic developments in the second half of the 20th century show us that rivalries and confrontations between superpowers were not only about possessing remarkable material resources, but also about the ability to dominate the international political scene through discourse, in other words, the ability to propose and popularize attractive ideas, values, and norms and to control political discourse on the international stage (Hlihor and Melinescu 2021; Ikenberry and Kupchan 1990, 283–315; Liao 2017, 110–133; Arquilla 1994, 24-30). Through communication mechanisms and means, a state imposes its status as a hegemonic power, managing

to convince, persuade, and compel other states to share its value system or to doubt their own criteria of knowledge, norms, or values. One such conflict, which has recently come to the attention of specialists in polemology and military strategy, is cognitive warfare. The human mind is a battlefield, with its entire arsenal of perceptions and representations of socially constructed reality, in particular, but also of the factual reality in which the individual moves. The goal of the belligerents is to change the way their opponents perceive reality and to orient them toward the dominant ideas and beliefs in their own society (Pripoae-Șerbănescu 2023, 261-280; Chiriac 2021, 55-71). Through these operations, powerful actors can change attitudes, reshape knowledge systems, and alter societal consciousness, often guiding people toward specific ideological or strategic goals. By manipulating the mental landscape, this form of warfare creates new opportunities for influence in the digital age. Although many specialists define this type of conflict as specific to the century of the digital revolution, the phenomenon is not new. The confrontation between the USSR and the US in the final period of the Cold War was not decided in the classic theatre of operations, but by conquering the minds of people living under the communist totalitarian regime (Hlihor and Melinescu 2021, 18-53). Some analysts argue that cognitive warfare is only one part of hybrid warfare, but it stands out because it focuses directly on the minds and behaviour of a target audience (Vakhshtain 2023). However, the same can be said about propaganda during the two world wars, and there are no studies that clearly define, from a conceptual point of view, the difference between propaganda, psychological warfare, info-ops (Hentea 2008), or, more recently, cognitive warfare. There is no widely accepted definition among specialists regarding cognitive warfare. Despite the valuable efforts of researchers and practitioners, the concept of cognitive warfare has remained vague and closely linked to broader discussions about irregular warfare within military and intelligence communities (Nicholson 2001, 3-4). Therefore, we believe it is important to identify the elements that make up the cognitive battlefield. According to Polish military analyst Tomasz Gergelewicz, it is important to understand the components of 'cognition'. 'The cognitive dimension includes, among others, cultural beliefs, norms, motivation, emotions, vulnerabilities, identity, ideology, perception, will, awareness, attitude, understanding, opinions, experience, knowledge, assumptions, and behaviour. Defining these factors in a given environment is crucial for understanding by which means adversaries influence the minds of the target audience' (Gergelewicz 2024, 33). The cognitive dimension matters for both offensive and defensive operations. The mental strength of the parties in conflict, their understanding of objectives, and their will to survive constitute a hidden power of cognition, and the effectiveness of educational actions carried out in the realm of values and patriotic and civic consciousness depends exclusively on this power. If the cognitive dimension is at a low level, it can become a platform for hostile operations, and these operations can be instruments of expansion or even transformation of the perspectives, values, and interests of target groups. They arise from a deep knowledge of the mental space of certain target groups and societies and an understanding of how social and mental vulnerabilities can be exploited' (Gergelewicz 2024, 33).

Although, in theory, the use of cognitive warfare means and techniques should not differ from one country to another, it can be observed, for example, that 'The PRC's cognitive warfare methods go beyond NATO's recognised pillars and include gaining undue influence. Undue influence should be recognised as one of the pillars of the PRC's cognitive warfare operations. For instance, American investors in TikTok have been co-opted into becoming de facto lobbyists for PRC interests, and they have significant leverage in politics and business. The PRC seeks to co-opt politicians and government leaders into serving their interests and promoting PRC messaging' (Davis 2025). Concerns about forms of cognitive warfare have also grown in the Russian Federation, especially since the outbreak of the war in Ukraine. According to sociologist Viktor Vakhshtayn (listed by the Russian Federation's Ministry of Justice as a foreign agent), cognitive warfare has three layers. The first layer/dimension, the most superficial, is a war of narratives, a clash of different stories. Stories in the military sphere can have varying degrees of emotional charge and persuasive power (Vakhshtain 2023). The success of a cognitive warfare operation in this dimension depends on how credible the narrative is among the target audience. The second dimension of cognitive warfare, according to the Russian sociologist, is semantic in nature. 'It is a much more costly (and bloodier) undertaking than the war of narratives. There is a word whose use—regardless of narrative—can land you in a Russian prison. Ten years ago, in much calmer times, many journalists lost their jobs for using the phrase 'Primorski partisans' (Vakhshtain 2023). Ultimately, beneath the semantic and narrative layers lie what one of the founders of sociology, Emile Durkheim, called 'classification grids.' These are fundamental axioms that cannot be questioned or revised. In fact, these are the grids for reading the socially constructed reality of any society, which are the result of a long-term systematic education process involving the family, the church, traditions, etc., as well as the institutional side. They are concerned in particular with social-political, economic, and cultural-spiritual life. It is well known that at Yalta, the three great leaders of the Coalition of Nations during World War II agreed that, after the defeat of Nazi Germany, the European societies under Berlin's influence would be democratized. Did the three leaders have the same framework for building democracy? Certainly not. Stalin's was based on the ideology and values of Marxism-Leninism, while that of the Western leaders was based on the totally different values of liberal democracy.

As can be seen, regardless of the perspective from which cognitive warfare is defined, many of its objectives and goals overlap or interfere with those of public diplomacy. However, we cannot fail to notice a fundamental difference, generated precisely by the state of war that arises at a given moment between states. In times of peace, the public diplomacy of a state/government can communicate directly with foreign audiences to establish a dialogue that informs and influences, with the aim of getting these foreign audiences to support a particular objective or policy of that state/government in another country. After the large-scale invasion of Ukraine in February 2022, the Russian authorities have shuttered the country's last independent media outlets, banned platforms such as Facebook and Twitter, and implemented

laws that make free speech – in the form of anti-war statements – punishable by as much as 15 years in prison. So far, the regime has arrested more than 15,000 people for demonstrating against the war, which is acting as a powerful deterrent. For those willing to risk arrest, censorship makes it difficult to discover how many others share their opposition to the war, and hinders the organisation of protests (European Council on Foreign Relations 2022). Since February 2026, WhatsApp is also blocked by Roscomnadzor (the Russian Authority for Regulating the Internet) because Meta, the American social media giant that owns it, refuses to store user data in the country. As early as March 2022, Meta was declared by the Kremlin `an extremist organization` which promoted Russophobia. On the other hand, Max, the local messaging service which comes preinstalled on all new devices, is aggressively promoted via billboards, TV ads, as well as in Russian mass media, as part of an ample campaign to replace foreign platforms. Max, an all-in-one app similar to WeChat from China, combines messaging, paid calls, and other services, allowing users to authenticate their identity with governmental platforms that offer public services. Serious questions are raised regarding the safety and confidentiality of user data on Max, as long as the app has excessive capacities for tracking and does not have adequate encryption (Chia and Tavener 2026).

Under these circumstances, Western public diplomacy is only possible in societies that reject war and military aggression against another state. On the other hand, even the state considered to be the aggressor no longer has the opportunity to promote its image and interests in states that condemn and oppose military aggression. The European Council has suspended since March 2022 the broadcasts of Sputnik and Russia Today radio stations in the EU, in the wake of the Russian Federation's aggression in Ukraine. Both stations bolster the systematic international campaign of the Russian state to misinform, manipulate information, and distort facts to justify and support the military aggression in Ukraine and to consolidate the strategy to destabilize neighbouring countries, EU member states (Council of the EU 2022). Under such circumstances, it is difficult to talk about communicating and informing a foreign audience, rather about hitting a wall as researcher Carlos Solar states: 'Russia and the West have gradually engaged in a 'dialogue of the deaf', with public diplomacy and cooperation being eliminated from the landscape' (Solar 2024). The battle to win the minds and hearts of a target audience through public diplomacy has been restricted to areas and regions considered neutral in relation to the war in Ukraine.

The battle between strategic narratives for credibility and legitimacy. Public diplomacy in 'neutral territories'

Strategic storytelling plays a key role in promoting the national image and interests through actions and means specific to public diplomacy. 'Strategic narratives are a means by which political actors attempt to construct a shared meaning of the past, present, and future of international politics to shape the behaviour of domestic

and international actors. They are a vital component of how states seek to establish and maintain influence in the world' (Miskimmon, O'Loughlin, and Roselle 2018, 4). Through public diplomacy, political actors often use strategic narratives to try to create a common understanding of the past, present, and future of world politics, intending to influence the actions of domestic and foreign actors. These play a crucial role in the efforts of states/governments to gain influence, legitimacy, and prestige in the international arena through public diplomacy. The essential condition is that strategic narratives be chosen that are appropriate for audiences in territories considered neutral in relation to an ongoing war, such as the war in Ukraine, because they will respond positively to the messages received or, conversely, ignore them. Therefore, researching the profile of the target audience regarding the reception of narratives offers more opportunities for a positive reception of the messages conveyed. This reduces the risk of miscommunication on the part of public diplomacy organizations and institutions.

Renowned specialists in international communication point out that 'In contrast to disinformation (deliberate lying) or misinformation (accidental lying), miscommunication is understood in terms of the complexity policy makers face in communicating with different publics and policy communities across the world. Perfect communication is impossible. Different societies already possess different narratives about how world order has emerged, each emphasising different events and often interpreting the same events in terms of different narrative trajectories or timelines' (Miskimmon, O'Loughlin, and Roselle 2018, 4). Their conclusion is that finding a common narrative between societies is difficult—but not impossible. One of the solutions for finding it is narrative credibility. Professors Robert H. Gass and Joh S. Seiter consider credibility to be a perceptual process. 'Whether a source possesses credibility or not defines credibility as 'judgements made by a perceiver' concerning the believability of a communicator, they say. They underline that 'credibility does not reside in a source. It is bestowed on a source by an audience' (Gass and Seiter 2020, 155-156). Joseph S. Nye reaches the same conclusion: Reputation has always mattered in world politics, but the role of credibility becomes an even more important power resource. Information that appears to be propaganda may not only be scorned; it may also turn out to be counterproductive if it undermines a country's reputation for credibility' (Nye Jr. 2019, 11). An obvious example is when the public diplomacy efforts of US organizations failed to counteract the decline in the credibility of the US administration in relation to the treatment of prisoners at Abu Ghraib and Guantanamo—in a manner incompatible with American values. The negative perception could not be reversed by broadcasting images of Muslims living well in the United States. Very little has been written in academic and public circles in our country about how credibility is achieved in public diplomacy actions and practices. When credibility on the international political scene is invoked, most often reference is made to the studies and works of Thomas Schelling (Schelling 2000). However, the renowned American professor refers to credibility in strategic negotiation in international politics. In this context, credibility refers to the

credibility of threats, promises, and commitments—it is linked to future events, in the sense that an actor in international politics tries to influence the other's perception of the consistency between present messages/commitments and future actions. But here too, issues arise regarding how much trust each party has in the other. The history of the 20th century has countless examples of written or verbal commitments that were not honoured. In achieving credibility through public diplomacy, things are very different from classical diplomacy. 'The stake is not the convergence on an agreement but rather the persuasion of a target audience' (Mor 2012, 397). The way in which these limits for narrative credibility have been surpassed in diplomatic practice in the case of armed conflict can be identified in the Russian-Ukrainian war that started in February 2022. Argumentation plays a decisive role in this situation because it matters whether the opposing party agrees with your ideas and opinions or not. Each of the two parties tries to convince the other of a certain thesis/opinion.

Gaining credibility for messages conveyed through public diplomacy actions to a target audience is an important step in gaining that audience's trust, especially today, when the world seems to have entered an era of mistrust (Cohen 2016), but also of a veritable information explosion due to the digital revolution. Joseph S. Nye Jr. emphasized that 'Technological advances have led to a dramatic reduction in the cost of processing and transmitting information. The result is an explosion of information, and that has produced a 'paradox of plenty'. Plenty of information leads to a scarcity of attention. When people are overwhelmed with the volume of information confronting them, it is hard to know where to focus. Attention, rather than information, becomes the scarce resource. Reputation becomes even more important than in the past, and political struggles occur over the creation and destruction of credibility, which is affected by social and political affinities (Nye Jr. 2019). Any public diplomacy organization/institution strives to achieve effective (i.e., persuasive) communication and, for this reason, attempts to build as solid a credibility as possible. However, practice in public diplomacy shows us that developing a plan that works (strategy development) and what actually works (the question of results) are not one and the same thing. Credibility does not come about by itself, 'naturally'. Being a perceptual product, it is achieved through interaction, which means that material, financial, and other resources alone are not enough. A message/narrative is also needed that speaks to the consumer's heart, sticks in their mind, and eventually spreads to others. From this point of view, it is also necessary to build a credibility strategy (Mor 2012, 395). Such a strategy must lead to surpassing the limits existing between the two societies in conflict. One of these limits refers to the very credibility of the message coming from the opposing society, which is almost by default relegated to disinformation, manipulation, and war propaganda. For this very reason, the public diplomacy organisations and institutions focus mainly on different target audiences in the international public opinion arena. Here as well, the public diplomacy practitioners who build such credibility strategies must take into account the limit engendered by the asymmetry between the two conflicting states. Although the most powerful has superior military power, the

constraints related to image coming from public opinion and the fear of international damnation often limit the operational freedom. This dynamic produces an effect of reversed asymmetry: the weaker players use mass media and images as weapons to attract sympathy, to mobilise international intervention, and to counterbalance their military inferiority (Yarchi 2025).

The way in which these limits for narrative credibility have been surpassed in diplomatic practice in the case of armed conflict can be identified in the Russian-Ukrainian war that started in February 2022. Russia's image in the eyes of foreign audiences is an aspect that must be taken into account when analysing Russian public diplomacy. While Russia's image as undemocratic, corrupt, and aggressive can be attributed to the Soviet image during the Cold War, the impact of foreign policy can be presented as significant in terms of low credibility. This brings us back to the discussion of the relationship between foreign policy and domestic policy, as well as the importance of co-optation rather than publicity in the field of public diplomacy. The Ukrainian conflict was an example that contributed to the image of an aggressive Russian Federation. The Russian occupation of Crimea has shattered its international image, which is seen as a rogue state by more and more countries and their citizens. Russia's image in the EU was consistently tarnished all the while Vladimir Putin was talking about the weakness of NATO's Eastern European partners in Poland, Romania, and the Baltic states (Tătar 2023, 82). The large-scale war against Ukraine made it impossible for public diplomacy to take any steps to restore Russia's image in the West and liberal democratic societies, due to its association with an aggressor state.

The collapse of the credibility of the narratives used by Russian public diplomacy for audiences in Europe and America has led Moscow to turn its attention to other regions, such as Latin America, Asia, and Africa (Solar 2024). To achieve its public diplomacy goals in Latin American countries, it mainly uses news agencies to support the Kremlin's so-called 'special military operation' in Ukraine, openly challenging dissenting opinions. It also uses the local press, where Russian diplomats accredited in these countries publish articles justifying military aggression and condemning the West for so-called anti-Russian actions. In Mexico, for example, Ambassador Nikolay Sofinsky wrote an editorial in La Jornada in September 2023 criticising the West for 'using energy as a weapon' and causing turmoil in international hydrocarbon trade through 'illegitimate restrictions and anti-market measures'. For the Russians, it may be a favourable factor that Mexican President Andrés Manuel Lopez Obrador has not taken a direct position in the conflict between Moscow and Ukraine (Solar 2024). Although the effectiveness of such activities in Latin American countries is unclear (Berg, Hidalgo and Ziemer 2025), leaders in Moscow insist on turning public diplomacy tools into disinformation campaigns that exploit the openness of democratic societies (Dunn 2025). 'RT en Español and its partner in crime, Sputnik Mundo, have embedded themselves across Latin America under the guise of alternative media. Their sleek production and emotionally charged content often present themselves as a counterbalance to Western influence. RT claims to be

the most-viewed international news channel in the world. At first glance, it seems to be just another successful world news network. However, their front-page articles weave misleading and critical narratives of U.S. foreign policy into their coverage of current events in Latin America. Their attempt at subtlety is strikingly obvious' (Dunn 2025). Ukraine, although not a minor power in international politics, has also played an excellent part with the help of public diplomacy. It has built an efficient public diplomacy strategy to bolster the engagement to fight for independence and Western democratic values, maintaining at the same time its credibility and encouraging international support. The Ukrainian case shows that narratives focused on resilience and common democratic values can efficiently counter contradictory messages, avoiding the risks of excessively negative or unidirectional approaches (Bjola and Fjällhed 2025, 2059–2083).

Conclusions

Since society has entered the digital revolution era characterized by geopolitical and geostrategic dynamics unprecedented in history, the communicational environment of public diplomacy has suffered essential changes. Once dominated by cultural exchanges, radio broadcasts, and carefully elaborated discourses, it now promotes – and faces – the dynamics of digital instruments which, on the one hand, have brought along good things such as speed and volume of communication and, on the other hand, negative effects which seriously affect the credibility of the narratives used by public diplomacy. Today, digital platforms such as Twitter, TikTok, and LinkedIn have transformed the practitioners of public diplomacy into participants in global conversations.

Since neoclassical forms of war have become prominent and the rapid spread of information via social media platforms raises doubts about the credibility of traditional diplomatic efforts, the importance of building trust via means and forms of public diplomacy characterized by transparency, empathy, and involvement has never been more apparent. Analyses and research in this field show that fake narratives and the deepfake phenomenon will not decrease in the near future due to the dialogue of public diplomacy organisations with foreign audiences. Consequently, the role of the digital revolution in public diplomacy cannot be overestimated or underestimated with regard to the credibility of the narratives specific to public diplomacy.

The present study aims to draw attention to the fact that it is important that we understand the objective and subjective factors that lead to the increase/decrease of credibility of the narratives of public diplomacy. In today's interconnected world and in the post-truth era, the winning narratives of any form/action of public diplomacy are those that conquer the mind and soul of the target audience. This can, in turn, become one of the main communicative actors of public diplomacy, creating and distributing narratives online in a totally independent fashion. Online

communication has transformed the global audience into a communicative sphere in which billions of narrators work together by sharing cultural knowledge and attitudes. The actions and activities run by public diplomacy organisations and institutions will thus be able to surpass more easily the limits that affect credibility in international communication.

References

Arquilla, John. 1994. "The Strategic implications of strategic dominance". *Strategic Review* 22(3): 24-30.

Berg, Ryan C., Natalia Hidalgo, and Henry Ziemer. 2025. "How Does Latin America and the Caribbean View the Ukraine Conflict After Three Years of War?" *Center for Strategic and International Studies*, February 24. https://www.csis.org/analysis/how-does-latin-america-and-caribbean-view-ukraine-conflict-after-three-years-war.

Bjola, Corneliu, and Alicia Fjällhed. 2025. Public diplomacy in the crossfire: decoding Ukraine's 'Strategic Self' during wartime. *International Affairs* 101(6): 2059–2083. https://academic.oup.com/ia/article/101/6/2059/8292954.

Chia, Osmond, and Ben Tavener. 2026. "Russia orders block on WhatsApp in messaging app crackdown". https://www.bbc.com/news/articles/clygd10pg5lo.

Chiriac, Olga R. 2021. „Războiul cognitiv în competiția marilor puteri ale secolului al XXI-lea: încadrarea activității militare în Marea Neagră". *Gândirea Militară Românească.* https://doi.org/10.55535/GMR.2021.4.02.

Cohen, Roger. 2016. "The Age of Distrust". *The New York Times*, 21 Sep 2016. https://www.nytimes.com/2016/09/20/opinion/the-age-of-distrust.html.

Council of the EU. 2022. "EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik`s broadcasting in the EU". https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/.

Davis, Johnny B. 2025. *Chinese Strategic Cognitive Warfare Use of TikTok and Social Media*. Helms School of Government Public Policy Conference 2025. https://digitalcommons.liberty.edu/cgi/viewcontent.cgi?article=1007&context=hsgppconference.

Dunn, Jeremy. 2025. "Sabotaging Truth: Russia and China's attempt to control Latin America". *Modern Diplomacy*, August 14. https://moderndiplomacy.eu/2025/08/14/sabotaging-truth-russia-and-chinas-attempt-to-control-latin-america/.

European Council on Foreign Relations. 2022. *Putin's war at home: Censorship and disinformation*, 2 June. https://ecfr.eu/article/putins-war-at-home-censorship-and-disinformation/.

Gass, Robert H., and John S Seiter. 2020. "*Credibility and Public Diplomacy*", in N. Snow, P. M. Taylor, Eds., *Handbook of Public Diplomacy,* 2nd Edition, Routledge. https://www.routledge.com/Routledge-Handbook-of-Public-Diplomacy/Snow-Cull/p/book/9781138610873.

Gergelewicz, Tomasz. 2024. "Countering Disinformation Concept for building social resilience in times of cognitive warfare". *Defence Science Review***,** no. 20: 31-44. https://doi.org/10.37055/pno/200300.

Hentea, Călin. 2008. *Noile haine ale propagandei*. București. Editura Paralela 45.

Hemingway, Albert. 1994. "Our War Was Different: Marine Combined Action Platoons in Vietnam". Annapolis. Naval Institute Press MD.

Hess, Gary H. 2015. *Vietnam: Explaining America's Lost War,* 2nd Edition. Wiley-Blackwell.

Hlihor, Constantin, and Mihail Andi Băncilă. 2024. "Vin vechi în sticle noi". Războaiele contemporane între realitatea concretă (acțiune umană specifică) și realitatea social construită (concepte, teorii, strategii, modelare și simulare)". *Punctul Critic* nr. 3-4 (49-50).

Hlihor, Constantin, and Nicolae Melinescu. 2021. *TVR ¨– Actor și martor la prăbușirea comunismului și naşterea democraţiei.* București. EIKON.

Hlihor, Ecaterina. 2023. "Public diplomacy during military international conflicts. The Ukraine war case". *Bulletin of "Carol I" National Defence University* 12(1): 19-30. https://doi.org/10.53477/2284-9378-23-02.

Ikenberry, G. John, and Charles A. Kupchan. 1990. "Socialization and hegemonic power". *International Organization* 44(3): 283-315. https://doi.org/10.1017/S002081830003530X.

Liao, Ning. 2017. "The Power of Strategic Narratives, The Communicative Dynamics of Chinese Nationalism and Foreign Relations", in Alister Miskimmon, Ben O'Loughlin, and Laura Roselle, eds., *Forging the World: Strategic Narratives and International Relations.* Michigan University of Michigan Press, Ann Arbor.

MEMORANDUM for Director of Central Intelligence. 1968. SUBJECT. New Book: *The Betrayal* by Lt. Col. William R. Corson, USMC (ret.). https://www.cia.gov/readingroom/docs/CIA-RDP80B01676R001600030006-8.pdf.

Miskimmon, Alister, Ben O'Loughlin, and Roselle, Laura. 2018, "Strategic Narrative: 21st Century Diplomatic Statecraft / Narrativa estratégica : el arte de la diplomacia en el siglo XXI". *Revista Mexicana de Política Exterior*, no. 113. https://revistadigital.sre.gob.mx/images/stories/numeros/n113/miskimmonoloughlinrosellei.pdf.

Mor, Ben D. 2012. "Credibility talk in public diplomacy". *Review of International Studies* 38(2): 393-422. https://doi.org/10.1017/S0260210511000489.

Müller, Leonie. 2022. *Putin's war at home: Censorship and disinformation.* European Council on Foreign Relations, 2 June. https://ecfr.eu/article/putins-war-at-home-censorship-and-disinformation/.

Nicholson, Michael. 2001. C. *The Cognitive Battlefield: A Framework for Strategic Communications*. Kansas. School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth.

Nye Jr., Joseph S. 2019. "Soft Power and Public Diplomacy Revisited". *The Hague Journal of Diplomacy* no. 14. https://brill.com/view/journals/hjd/14/1-2/article-p7_2.xml?srsltid=AfmBOortn0OxiZo2hYfRYOi41cDxGci2bmH4KvNIqwASZ85n_HUx48Wg.

Peterson, Michael. 1989. *The Combined Action Platoons: The U.S. Marines' Other War in Vietnam*. New York City. Praeger.

Pripoae-Șerbănescu, Ciprian. 2023. "Războiul cognitiv – dincolo de manevre, dominație și informații – o confruntare pentru viitorul imaginat". *Conferința Științifică Internațională Gândirea Militară Românească*. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2023%20gmr/Proceedings%202023/PRIPOAE-SERBANESCU.pdf.

Saliu, Hasan. 2023. "Narratives of Public Diplomacy in the post-Truth Era: The decline of Soft Power". *Communication & Society* 36 (2): 209-224. https://revistas.unav.edu/index.php/communication-and-society/article/view/43702/37164.

Schelling, Thomas C. 2000. *Strategia conflictului*, traducere de Elena Burlacu și Ruxandra Toma. Bucuresti: Editura Integral.

Solar, Carlos. 2024. "Moscow's Other Offensive: Russian Public Diplomacy in Latin America". *RUSI*, 19 March. https://www.rusi.org/explore-our research/publications/commentary/moscows-other-offensive-russian-public-diplomacy-latin-america.

Sukhorolskyi, Petro, and Iryna Sukhorolska. 2024. "The public diplomacy of Ukraine in wartime: a path to reputational security. *Eastern Journal of European Studies* vol. 15 (SI). https://ejes.uaic.ro/articles/EJES2024_15SI_SUK.pdf.

Tătar, Adriana Camelia. 2023. "Public Diplomacy of The Russian Federation in the International Relations". *Studia-Securitatis*, no.1. https://magazines.ulbsibiu.ro/studiasecuritatis/wp-content/uploads/STUDIA-SECURITATIS-NO.1-2023-77-87.pdf.

Vakhshtain, Viktor. 2023. „Историю пишут не победители. Ее пишут дети победителей. А дети далеко не всегда на стороне родителей". Istoriyu pishut ne pobediteli. Ee pishut deti pobediteley. A deti daleko ne vsegda na storone roditeley. *Polit.ru*, Декабрь 21, 2023. https://polit.ru/articles/posle/viktor-vakhshtayn-istoriyu-pishut-ne-pobediteli-ee-pishut-deti-pobediteley-a-deti-daleko-ne-vsegda-n/.

Yarchi, Moran. 2025. "Strategic narratives as an image war tool". *Place Brand Public Diplomacy*. https://doi.org/10.1057/s41254-025-00418-0.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania

Mihail-George GURANDA*
Dănuț MAFTEI, Ph.D.**

*Senior Legal and Regulatory Affairs Expert | EU-Level Cybersecurity Policy Specialist | Strategic Advisor in Public Policies
e-mail: mihaigu@riseup.net
**National Cyber Security Directorate, Bucharest, Romania
e-mail: dn.maftei@gmail.com

Abstract

This article examines the relationship between Cyber Warfare, security culture, and organizational resilience in Romania through the interaction of the legal framework, institutional architecture, and public governance practices. In the context of expanding hybrid conflicts and the convergence of technical, strategic, and cognitive threat dimensions, security culture can no longer be treated as a secondary issue, but as a condition for organizational and state resilience. Methodologically, the study relies on qualitative research combining doctrinal analysis, legal-institutional analysis, and a case study of Romania, drawing on relevant national legislation, the European Union acquis, institutional documents issued by DNSC, ENISA, and NATO, as well as relevant academic literature. The central argument is that Romania's recently developed normative and institutional architecture, particularly Law no. 58/2023, G.E.O. no. 155/2024, the operationalization of SNAC, and integration with NIS2 mechanisms, creates premises for strengthening security culture and resilience, without automatically guaranteeing the internalization of security behaviours.

Keywords:
Cyber Warfare; Security Culture; Cybersecurity; Cyber Defense; Cyber Crisis; Threats; Resilience; Cyber Governance.

Article info
Received: 13 February 2026; Revised: 23 February 2026; Accepted: 17 March 2026; Available online: 8 April 2026

Citation: Guranda, M.G., and D. Maftei. 2026. "Security Culture and Organizational Resilience in the Context of Cyberwarfare: the Case of Romania." *Bulletin of "Carol I" National Defence University* 15(1): 252-265. https://doi.org/10.53477/2284-9378-26-15

Introduction

Over the past decade, cyber warfare has profoundly altered the way states perceive the relationship between security, conflict, and the functioning of public institutions. Unlike traditional cyber threats, which are primarily associated with criminal activities or the technical protection of networks, cyber warfare is part of a broader strategic framework in which digital operations can be used for espionage, disruption of critical services, coercion, foreign influence, and the erosion of public trust in democratic institutions (Lin 2012).

An analysis of threats attributed to APT (*Advanced Persistent Threat*) groups illustrates the high degree of sophistication of cyber operations carried out by various state actors. Thus, the APT43 group (alias *Kimsuky*), supported by North Korea, has become a symbol of this evolution, carrying out complex espionage and strategic intelligence-gathering activities in the diplomatic, technological, and defense sectors (Mishra 2025). This malicious group combines advanced persistence techniques with the exploitation of legitimate operating system tools, bypassing conventional detection methods and targeting government institutions, think tanks, research centers, and critical information infrastructure in EU member states (MS), the United States, Japan, and South Korea.

A similar trend can be observed in the capabilities of the Russian group *Curly COMrades* (Lyons 2025), which uses virtualization technologies to hide malicious code within an isolated environment, drastically reducing the likelihood of detection. This offensive innovation demonstrates the creative use of legitimate technologies for hostile purposes and marks a shift in the defensive paradigm: simple endpoint-level detection becomes insufficient in the face of threats that exploit virtualized architectures and dynamic persistence mechanisms.

This transformation has direct consequences for security culture. In the classical paradigm, cybersecurity was frequently treated as a technical specialty. In contrast, in the current paradigm, it has become a matter of governance, organizational behavior, inter-institutional coordination, and societal resilience. Several reports highlight the fact that a mature cybersecurity culture involves not only rules and controls, but also values, attitudes, practices, and learning mechanisms that influence the actual behavior of organizational actors (Huang and Pearlson 2019).

In the case of Romania, this evolution is particularly relevant. The transition from a fragmented approach to cybersecurity toward a more coherent model of crisis governance and cyber alerting is indicated by:

- Recent legislative developments, such as Law No. 58/2023 on Romania's cybersecurity and cyber defense, and Government Emergency Ordinance (G.E.O.) No. 155/2024 establishing a framework for the cybersecurity of networks and information systems in the national civilian cyberspace (Romanian Government 2024);

• Institutional developments such as the establishment of the National Cyber Security Directorate (DNSC), the operationalization of the National Cyber Alert System (SNAC), as well as integration into the mechanisms of the Directive (EU) 2022/2555 - NIS2 (EUR-Lex 2022) and the *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe).

However, the existence of a more robust regulatory and institutional architecture does not automatically solve the central issue of resilience: the way in which rules, procedures, alert mechanisms, and inter-institutional cooperation are transformed into stable practices, organizational reflexes, and public trust. This is, in essence, the issue of security culture.

This paper begins with the following research question: **To what extent and through what mechanisms does Romania's regulatory and institutional framework for cybersecurity contribute to the development of a security culture and organizational resilience in the context of cyber warfare?**

In relation to this question, the article formulates three working hypotheses:

- Hypothesis 1: Normative clarity and the formal distribution of competencies enhance coordination capacity in cyber crises.
- Hypothesis 2: Alert mechanisms, inter-institutional cooperation, and public communication can foster the internalization of security behaviors.
- Hypothesis 3: In the absence of implementation indicators and systematic data on compliance and institutional learning, the effect of the legal framework on security culture remains plausible but only partially demonstrable.

Given the circumstances described, this article proposes, on the one hand, a conceptual reordering of the relationship between cyber warfare, security culture, and organizational resilience, and, on the other hand, it offers a structured analysis of the Romanian case, placing domestic regulatory and institutional developments within the context of the EU – NATO convergence and of the recent European requirements regarding the management of cyber incidents and crises.

1. Conceptual framework

Conceptual clarity is essential for any scientific analysis of cybersecurity. In the absence of a rigorous definition, terms such as "cyber warfare," "security culture," and "organizational resilience" tend to be used metaphorically or interchangeably, which affects both the coherence of the argument and the possibility of empirical evaluation.

1.1. Cyber Warfare

According to several reports, *Cyber Warfare* is not reduced to the mere existence of cyberattacks. It involves the use of cyber capabilities within a strategic logic of conflict, particularly by states or actors sponsored by various countries and governments, to produce negative political, military, economic, or psychological

effects on an adversary. Analyses of cyber conflicts highlight precisely the difficulty of separating the technical dimension of the attack from its strategic purpose and its effects on the political order and institutions (Sutton and Tompson 2023).
For this article, Cyber Warfare could be defined as the set of offensive, defensive, and influence operations conducted in and through cyberspace to impair the operational capacity, decision-making, trust, or resilience of a state, certain institutions, or critical information infrastructure. It takes place in the information environment, with actors and targets in both the physical and non-physical domains, and the level of violence may vary depending on the circumstances (Taddeo 2012). This definition allows for the inclusion of both the technical and the cognitive and institutional dimensions.

1.2. Security Culture

The concept of *Security Culture* must be distinguished from mere formal compliance. The relevant reports in the field specify that a security culture involves a set of shared values, beliefs, attitudes, and behaviors that influence the way in which members of an organization understand risks, respond to rules, and participate in the protection of digital assets. Recent models emphasize the link between culture and behavior, with education, leadership, group norms, communication, and reward systems directly influencing security conduct.
Security culture is defined in Romania by the *National Defense Strategy Guide for the period 2015-2019*. This document defines security culture as the totality of those values, norms, attitudes, or actions that determine a society's understanding and assimilation of the concept of security and its derivatives (national, international, and collective security; insecurity; security policies, etc.) (Presidency 2015). Thus, relevant actors (institutions, organizations, and citizens) perceive cyber risks, prioritize security, and act consistently to prevent, report, and manage incidents.
For this article, it is also important to highlight the existence of a *Cybersecurity Culture*, which is represented both by the norms and values that members of an organization hold regarding cybersecurity and by the way these are manifest in their behavior (Sutton and Tompson 2023).

1.3. Organizational Resilience

The concept of *Organizational Resilience* is frequently used in security discussions, but often without being operationalized. It is described in recent academic literature as a *multifaceted capability* that includes anticipation and preparation, endurance and response, recovery, and subsequent learning.
According to the definition provided by the British Standards Institution (BSI), organizational resilience is the ability of an organization to anticipate, prepare for, respond to, and adapt to sudden changes and disruptions in order to survive and thrive (Hilio 2025). In the case of Cyber Warfare, this entails flexibility, agility, and innovation in the face of challenges, as well as maintaining essential functions during a cyber incident, recovering within a reasonable timeframe, and integrating lessons learned into future policies, procedures, and architectures.

1.4. The Relationship Between Concepts

The relationship between the three concepts can be formulated as follows: *Cyber Warfare* represents the conflict environment and the type of strategic pressure; *Security Culture* represents the socio-organizational dimension through which actors perceive and internalize risk; *Organizational Resilience* represents the actual capacity to cope with disruption. In this context, security culture is not synonymous with resilience, but it constitutes one of the essential prerequisites for achieving it.

2. Methodology

The article employs a qualitative methodology structured around three complementary methods: doctrinal analysis, legal-institutional analysis, and case study. This methodological approach is appropriate because the research does not aim to statistically measure individual behaviors, but rather to examine the relationship between norms, institutions, coordination mechanisms, and security concepts within a specific national context.

The doctrinal analysis aims to define key concepts and situate them within the specialized literature on *Cyber Warfare, Security Culture*, and *Organizational Resilience*. The legal-institutional analysis examines the relevant legislation and documents that define competencies, alert mechanisms, and the coordination architecture at the national and European levels. The case study applies these frameworks to Romania, with a focus on the DNSC, SNAC, the Cyber Security Operational Council (COSC), the National Center for Cyber Security Crisis Management (CNGCSC), and integration with the European mechanisms provided for by the NIS2 Directive.

The analyzed corpus includes national legislation, administrative norms and methodologies, European documents, institutional sources from ENISA (ENISA 2026), DNSC (DNSC 2026) and NATO (NATO 2026b), as well as academic works relevant to security culture and resilience. From a research design perspective, Romania is treated as a "*most likely case*" for analyzing how legal and institutional consolidation can create the conditions for the maturation of security culture, without this automatically proving the existence of a fully empirically validated causal relationship.

To avoid speculative claims, this paper employs an explicit set of analytical criteria to assess the contribution of the regulatory and institutional framework to the culture of security and resilience: the clarity of roles and responsibilities; the existence of alert and escalation mechanisms (DNSC 2025); the capacity for inter-institutional coordination; the integration of public communication; the inclusion of exercises, planning, and learning; the alignment with European and Euro-Atlantic mechanisms.

The limitations of the research stem from the fact that the scientific study did not include interviews, sociological surveys, sets of quantitative indicators, or systematic comparisons across multiple countries. For this reason, conclusions regarding the effects on security culture are formulated cautiously, in terms of "institutional premises," "enabling mechanisms," or "conditions of possibility," rather than as definitive empirical demonstrations.

3. The European architecture of cyber resilience

In recent years, the European Union has shifted from an approach centered predominantly on technical cooperation to a more complex architecture for managing cyber incidents and crises (ENISA 2026). In this evolution, ENISA, the EU Network of *Cyber Security Incident Response Teams* (CSIRTs Network), and, more recently, EU-CyCLONe have become central elements of a multi-level governance framework oriented not only toward technical response, but also toward strategic coordination and shared situational awareness (EUR-Lex 2022).

The NIS2 Directive is particularly relevant, as it contains provisions that structure cooperation among EU MS around clearer obligations regarding risk management, incident notification, coordination, and preparedness. Article 16 of the NIS2 Directive establishes the role of EU-CyCLONe in the strategic coordination of large-scale cyber incidents and crises, complementing the more technical role of the CSIRTs Network.

This technical-strategic duality is important for the subject under study. It suggests that cyber resilience can no longer be reduced solely to the technical capability of detection and remediation (EUR-Lex 2024), but it also entails institutional mechanisms for interpretation, decision-making, communication, and cooperation across different levels of governance. From this perspective, the European model offers a useful framework for understanding how cybersecurity is progressively integrated into the broader logic of democratic and institutional resilience.

Furthermore, European initiatives regarding crisis exercises, the cybersecurity reserve, and cross-border interoperability point to a significant doctrinal shift: the focus is shifting from securing infrastructure to preparing public systems for continuity, cooperation, and recovery. This shift has direct consequences for EU MS, including Romania, as it compels national institutions to develop mechanisms that are compatible both technically and procedurally.

4. The Regulatory and Institutional Framework in Romania

4.1. From fragmentation to coordination

At the national level, recent developments point to a consolidation of the cybersecurity and defense architecture. Through G.E.O. No. 104/2021 (Art. 3(o) and

Art. 17) (Romanian Government 2021), the role of the DNSC in managing cyber crises during peacetime was strengthened, and the institutional foundations were laid for the operation of a national cyber security crisis management center.
Law No. 58/2023 has further developed this framework, establishing an integrated institutional framework for the management of cyber risks, incidents, and crises. From the perspective of this study, the law's significance lies not only in the introduction of obligations and competencies, but also in the formalization of a logic of strategic coordination among different institutional levels (Romanian Parliament 2023).
The role of the COSC, its relationship with the DNSC, and the Supreme Council for National Defense (CSAT) (CSAT 2026), as well as the mechanisms associated with cyber alert levels, indicate an attempt to overcome the traditional fragmentation of responsibilities. In analytical terms, this can be interpreted as a favorable condition for a security culture, as clarity of responsibilities and the existence of a decision-making chain reduce organizational ambiguity and increase the predictability of the response.

4.2. Operationalization of the SNAC

The implementation of the National Cyber Alert System, pursuant to DNSC Order No. 180/2024 approving the Methodology on cyber alert levels and procedures for action in cyber alert situations (DNSC 2024) is one of the most relevant aspects of the topic addressed in this article. The SNAC is not merely a technical tool for risk reporting, but also a mechanism with cultural and organizational potential, as it connects technical analysis, institutional decision-making, and public communication.
From the perspective of security culture, the relevance of SNAC stems from three elements: the standardization of the response through alert levels and associated action plans; the inclusion of private and sectoral actors in the logic of alerting and preparedness; and the public communication dimension, which creates the possibility of transitioning from exclusively technical governance to one that addresses social behaviors and perceptions.
However, it is important to make the following methodological clarification: the fact that the SNAC is designed to contribute to awareness and coordination does not automatically demonstrate its actual effect on security culture. In the absence of data regarding the public's understanding of alerts, the level of compliance among targeted actors, or the impact of exercises and notifications on behavior, the appropriate conclusion is that SNAC establishes a mechanism with the potential to foster a security culture, not that it has already demonstrably produced societal maturation.

4.3. Integration with European mechanisms

An important aspect of the Romanian case is synchronizing the national architecture with the mechanisms outlined in the NIS2 Directive. G.E.O. No. 155/2024 and its subsequent approval by Law No. 124/2025 (Romanian Parliament 2025) consolidated this synchronization by establishing DNSC as the national authority for managing cyber crises in peacetime and as the contact point for EU-CyCLONe.

In 2024, Romania demonstrated the practical application of this framework by activating the relevant procedures in the context of election security. In this context, the DNSC operated simultaneously in coordination with:

- ENISA, for strategic support and information-sharing tools;
- EU-CyCLONe, where the network level was escalated to *Warning Mode*, activating dedicated channels and operational cooperation;
- the ENISA Network of Liaison Officers (NLO Network), for briefings and information requests;
- EU CSIRTs Network, where the transition to *Alert Cooperation Mode* was discussed, and relevant technical data was shared.

This example is significant because it highlights the shift from mere legislative transposition to the operational use of cooperation channels.

From an analytical perspective, these aspects support the idea that resilience is not merely an internal attribute of the state but also the result of being part of a broader cooperative framework. In this sense, the culture of institutional security must also be understood as a culture of interoperability, information sharing, and shared reflexes for action (Cheng 2023).

From the same perspective, EU-NATO convergence complements the European dimension of cyber resilience. For Romania, NATO's relevance lies not only in the strictly military dimension but also in the civil–military integration of planning, exercises, and strategic risk assessment. Mechanisms such as the *Cyberspace Operations Centre* (CyOC), the *NATO Integrated Cyber Defence Centre* (NICC), and the *NATO Cooperative Cyber Defence Centre of Excellence* (CCDCOE) provide a useful framework for lessons learned, exercises, and doctrinal interoperability, while initiatives such as the *Defence Innovation Accelerator for the North Atlantic* (DIANA 2026) and the *NATO Innovation Fund* (NATO 2026a) indicate that technological innovation and cooperation with the civilian sector are becoming part of the broader ecosystem of defense and digital resilience (NATO 2025). In this sense, this convergence reinforces the idea of resilience as a product of multi-level cooperation, not just national capability.

4.4. Democratic oversight and constitutional legitimacy

The case law of the Constitutional Court of Romania (CCR) (CCR 2026) establishes a clear framework: **the security of networks and information systems is no longer a purely technical field, but one of general interest, closely intertwined with national security**.

This issue is relevant not only from a legal standpoint but also from a conceptual one. In Decision No. 17/2015 (CCR 2015), the Constitutional Court of Romania draws a clear political and institutional line: **the coordination of cybersecurity at the national level must be exercised by a civilian body, under democratic control, not by intelligence, law enforcement, or defense agencies**.

The choice of who coordinates cybersecurity at the national level matters for the security culture for at least two reasons. First, legitimacy and public trust can

be affected by perceptions of the institutions coordinating security. Second, a democratic security culture cannot be built sustainably outside the requirements of normative clarity, proportionality, and the protection of fundamental rights.
Therefore, the constitutional and conventional framework is not external to resilience but is part of its conditions. Resilience built through opaque, disproportionate, or insufficiently controlled measures can generate reactions of distrust that weaken the very security culture it claims to strengthen.

5. The impact on security culture and organizational resilience

Cyber warfare has effects that extend beyond the strictly technical realm of securing networks and information systems, influencing security culture, institutional coordination, and organizations' ability to function under pressure and in stressful conditions. In this context, organizational resilience must be understood not only as the ability to ensure operational continuity but also as the capacity to anticipate, absorb, adapt to, and integrate the lessons learned from cyber incidents, hybrid campaigns, and disruptions encountered at the strategic level. In Romania's case, recent legislative and institutional developments suggest a shift from a predominantly technical approach to one of strategic governance, in which security culture becomes the connecting variable between norms, institutions, and organizational behaviors.

5.1. From technical protection to organizational security culture

One of the main consequences of cyber warfare is the shift in emphasis from exclusively technical protection toward organizations' ability to react coherently and adaptively under conditions of persistent stress. Sophisticated attacks, supply chain exploitation, and influence campaigns show that vulnerability stems not only from a lack of technical controls but also from deficiencies in coordination, communication, and institutional learning. From this perspective, a security culture entails more than formal compliance: it involves organizational reflexes, clear decision-making, and the transformation of rules into repetitive and internalized practices.

5.2. Institutional architecture and its impact on resilience

In Romania, Law No. 58/2023, G.E.O. No. 155/2024, the operationalization of the SNAC, and the integration with NIS2 mechanisms create important conditions for strengthening organizational resilience. This framework reduces fragmentation, clarifies roles, and introduces a logic of alerting, escalation, and coordination that can standardize the institutional response in crisis situations. However, the relationship between institutional architecture and security culture must be framed cautiously: the existence of procedures and competencies is a necessary condition, but not sufficient proof that organizations have internalized stable security behaviors.

5.3. The Societal and Cognitive Dimensions of Security Culture

The impact of cyber warfare is not limited to institutions but extends to how society

perceives risk and reacts to digital crises. In practice, the most significant effects occur when cyber incidents are accompanied by disinformation, information pressure, and the erosion of trust in institutions (Maftei 2025). In this context, the public communication component associated with SNAC is important because it can support faster and more proportionate responses, without, however, automatically transforming cybersecurity into a mature societal culture. The outcome will depend on the continuity of communication, institutional credibility, and the public's ability to interpret risk signals (Fomnya 2024).

5.4. The skills, the human factor, and the challenge of the Artificial Intelligence era

Another major effect of the transformation of the security environment is the growing importance of digital skills. The accelerated integration of Artificial Intelligence (AI) into operational and decision-making processes compels organizations to simultaneously manage classic cyber risks and risks associated with the interaction between people, data, and automated systems (Palma 2026). In this context, resilience depends not only on technology but also on having personnel capable of understanding the limits of automation, critically using digital tools, and maintaining human control over sensitive processes (Maftei 2024).

5.5. Implications for Romania

For Romania, the impact of cyber warfare on security culture and organizational resilience must be understood at the intersection of governance, administrative capacity, and professional training. The recent regulatory framework, the role of the DNSC, the functioning of the SNAC, and European interoperability provide a more robust coordination infrastructure than in the previous phase, but its lasting effect depends on recurring exercises, evaluation, continuous training, and the integration of lessons learned into institutional practices.

Consequently, strengthening the security culture cannot be treated as an automatic result of legislative reform, but rather as a continuous process of operationalization, coordination, and learning. This process requires clear planning mechanisms, the distribution of responsibilities among public and private actors, and the transformation of legal norms into verifiable organizational routines.

In practical terms, developing organizational resilience requires the consistent implementation of crisis planning, the regular conduct of interagency exercises, the integration of lessons learned into procedures, and the strengthening of public communication during alerts. At the same time, responsibility does not lie exclusively with central authorities but must be shared among competent public institutions, operators of essential services, private organizations, and actors involved in professional training.

In this context, a culture of security functions not merely as a regulatory requirement, but as a social and organizational practice, dependent on the continuity of institutional operations, the clarity of the decision-making chain, and the ability of relevant actors to cooperate under conditions of pressure and uncertainty.

Precisely for this reason, the essential step for Romania is not merely to strengthen the legal framework but to transform it into an effective mechanism for adaptation, coordination, and resilience.

Conclusions

This analysis shows that Romania is in a phase of significant regulatory and institutional consolidation in the field of cybersecurity and cyber defense. Recent legislative and administrative developments indicate the existence of a clearer architecture for European alerting, coordination, and interoperability compared to the previous period, particularly through the role of the DNSC, the operationalization of the SNAC, and integration into the mechanisms associated with the NIS2 Directive.

The answer to the research question is, however, nuanced. Romania's regulatory and institutional cybersecurity architecture contributes to the development of a security culture and organizational resilience by clarifying roles, standardizing alerts, strengthening coordination, and connecting to European and Euro-Atlantic cooperation networks. However, these developments must be interpreted cautiously. They create solid premises for strengthening security culture, but do not, by themselves, equate to demonstrating full internalization of security behavior at the organizational and societal level.
The main finding of the scientific study is, therefore, conditional. Romania has more robust legal and institutional foundations for strengthening resilience, but the lasting effects of this framework remain dependent on the implementation and transformation of norms into stable institutional practices.

The study also suggests that organizational resilience should be viewed within a broader framework than that of technical security. It includes institutional coordination capacity, public communication, European and Euro-Atlantic interoperability, as well as the preparation of a workforce capable of operating in an environment characterized by the convergence of cyber threats, information pressure, and the widespread use of AI.

In terms of public policy, four priority areas emerge. **The first** of these relates to the development of maturity indicators for security culture and organizational resilience in the public sector and in critical sectors. **The second** priority area concerns the strengthening of national exercises and interoperability with European and NATO mechanisms, with the integration of lessons learned into the regulatory and operational cycle. **The third** priority area is the one of strengthening public communication and digital literacy, with a focus on prevention and proportionate response. **The fourth** one involves adapting professional training to the new risks associated with the use of AI, automation, and human-system interaction in critical processes.

Therefore, the main challenge for cybersecurity and cyber defense in Romania is not merely the development of superior technical capabilities, but transforming these into an institutional and organizational culture robust enough to support resilience in a persistently contested strategic environment.

References

CCR. 2015. „Decizia nr. 17 din 21 ianuarie 2015 asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României." https://www.ccr.ro/wp-content/uploads/2020/07/Decizie_17_2015.pdf.

___**.** 2026. *Curtea Constituțională a României.* https://www.ccr.ro/.

Cheng, Joseph. 2023. „Building Cyberresilience From Collaborative Culture." *ISACA*. https://www.isaca.org/resources/isaca-journal/issues/2023/volume-3/building-cyberresilience-from-collaborative-culture.

CSAT. 2026. *Consiliul Suprem de Apărare a Țării.* https://csat.presidency.ro/.

DIANA. 2026. *Defence Innovation Accelerator for the North Atlantic.* https://www.diana.nato.int/.

DNSC. 2024. *ORDIN nr. 180 din 21 februarie 2024 pentru aprobarea Metodologiei privind nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică.* https://legislatie.just.ro/Public/DetaliiDocument/279736.

___. 2025. „Raport anual de activitate 2024." https://www.dnsc.ro/vezi/document/dnsc-raport-anual-2024.

___. 2026. *Directoratul Național de Securitate Cibernetică.* https://www.dnsc.ro/.

ENISA. 2026a. *EU incident response and cyber crisis management.* https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management.

___**.** 2026b. *European Union Agency for Cybersecurity.* https://www.enisa.europa.eu/.

EUR-Lex. 2022. „Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune." https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

___**.** 2024. „Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale." *Cyber Resilience Act.* https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng.

Fomnya, Hyelda Joseph. 2024. „The Influence of Cybersecurity. Risk Management Practices on Organizational Resilience." *Hallford Education.* https://hallford.education/wp-content/uploads/2026/01/The-Influence-of-Cybersecurity-Risk-Management-Practices-on-Organizational-Resilience.docx.pdf.

Hilio. 2025. *Reziliența individuală și organizațională – Definiție, rol și strategii de dezvoltare.* https://hilio.com/ro/blog/humancapital/ce-este-rezilienta-organizationala.

Huang, Keman, and Keri Pearlson. 2019. "For What Technology Can't Fix:Building a Model of Organizational Cybersecurity Culture." *Proceedings of the 52nd Hawaii International Conference on System Sciences.* doi:https://doi.org/10.24251/HICSS.2019.769.

Lin, Herbert. 2012. „Cyber conflict and international humanitarian law." *International Review of the Red Cross* 94 (886): 515-531. https://international-review.icrc.org/sites/default/files/irrc-886-lin.pdf.

Lyons, Jessica. 2025. *Russian spies pack custom malware into hidden VMs on Windows machines.* https://www.theregister.com/2025/11/04/russian_spies_pack_custom_malware/?cid=soc%7Cn%7Csprout%7Cemp&blaid=8069358.

Maftei, Dănuț. 2024. „The Cyber Competences Act - a Vital EU Regulation Concerning Mandatory Certification of Critical Network and Information Systems' Operators across the European Union." *Informatica Economică* 28 (2): 45-60. doi:10.24818/issn14531305/28.2.2024.04.

___. 2025. „"Three Warfares" versus "Hybrid Warfare". New Generation Warfare – New Approaches and Challenges." *Revista GeoPolitica.* https://www.geopolitic.ro/in/topics/geointellicence/page/2/.

Mishra, Siddhant. 2025. *Inside the Shellcode: Dissecting North Korean APT43's Advanced PowerShell Loader.* https://systemweakness.com/inside-the-shellcode-dissecting-north-korean-apt43s-advanced-powershell-loader-e6c51b77f486.

NATO. 2026a. *NATO Innovation Fund.* https://www.nif.fund/.

___. 2026b. *North Atlantic Treaty Organization.* https://www.nato.int/en.

___. 2025. „Request for Information (RFI) to engage with industry, academia and nations." https://www.act.nato.int/wp-content/uploads/2025/12/rfi025112.pdf.

Palma, Bryan. 2026. *The cybersecurity paradox: training the next generation workforce.* https://www.weforum.org/stories/2026/01/cybersecurity-paradox-training-the-next-generation-workforce/.

Presidency. 2015. „Ghidul Strategiei Naționale de Apărare a Țării pentru perioada 2015-2019." https://www.presidency.ro/ro/presa/securitate-nationala-si-aparare/ghidul-strategiei-nationale-de-aparare-a-tarii-pentru-perioada-2015-2019.

Romanian Government. 2021. *ORDONANȚĂ DE URGENȚĂ nr. 104 din 22 septembrie 2021 privind înființarea Directoratului Național de Securitate Cibernetică.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/246652.

___. 2024. *Ordonanță de urgență nr. 155 din 30 decembrie 2024 privind instruirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.* https://legislatie.just.ro/Public/DetaliiDocumentAfis/293121.

Romanian Parliament. 2025. *Lege nr. 124 din 7 iulie 2025 pentru aprobarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil.* https://legislatie.just.ro/public/DetaliiDocument/299675.

___. 2023. *Lege nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.* https://legislatie.just.ro/Public/DetaliiDocument/265677.

Sutton, Anna, and Lisa Tompson. 2023. "Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review." https://doi.org/10.31234/osf.io/h4uby.

Taddeo, Mariarosaria. 2012. „An analysis for a just cyber warfare." *2012 4th International Conference on Cyber Conflict (CYCON 2012).* Tallinn, Estonia. https://ieeexplore.ieee.org/document/6243976.

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)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 07.04.2026
The publication consists of 266 pages.