# BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 2/ 2025

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, 2025

## 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. 2/2025*

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Mechanisms of Disinformation Amplification in Hybrid Warfare: The Case of the Conflict in Ukraine

**Master's student Rafał ROMAŃSKI***
*The Józef Goluchowski University of Applied Sciences, Poland
e-mail: romanski@goluchowski.edu.pl

## Abstract

This article presents an interdisciplinary analysis of disinformation amplification mechanisms within the context of contemporary hybrid warfare, with particular emphasis on the armed conflict in Ukraine. The study aims to identify and characterize the complex processes that amplify false narratives, influencing both social perception and the informational environment. The main research question posed is: What disinformation amplification mechanisms are employed under conditions of hybrid warfare, and how do they affect the shaping of public awareness and conflict perception? The methodology combines qualitative content analysis, source triangulation, and network analysis of selected case studies, including manual analysis of hashtags and discussion groups. These include instances of denialism related to the Bucha massacre, heroic mythology (the "Ghost of Kyiv"), false flag operations (Zaporizhzhia Nuclear Power Plant), amplification on TikTok and Telegram, the functioning of botnets, and #IStandWithRussia campaigns. The findings indicate that disinformation is not a one-off communicative act but an iterative structure supported by three interrelated domains: propaganda communication, cognitive psychology, and algorithmic technologies. In conclusion, the research question is addressed, and five strategic action areas are proposed: media literacy education, cooperation with digital platforms, international coordination, support for independent media, and the development of cognitive resilience within society. The article contributes a novel theoretical framework in the form of a "hybrid tripartite model" (communication–perception–algorithms), which may serve as a useful analytical tool in future studies of disinformation in conflict situations.

**Keywords:**
disinformation; hybrid warfare; TikTok; propaganda; social perception; informational narratives; content analysis; fake news; algorithms; campaigns.

**Article info**
Received: 2 May 2025; Revised: 30 May 2025; Accepted: 3 June 2025; Available online: 27 June 2025

Citation: Romański, R. 2025. "Mechanisms of Disinformation Amplification in Hybrid Warfare: The Case of the Conflict in Ukraine." *Bulletin of "Carol I" National Defence University*, 14(2): 7-32. https://doi.org/10.53477/2284-9378-25-13

With the onset of the Russian Federation's armed invasion of Ukraine in February 2022, an intensified and coordinated disinformation campaign was observed, constituting an integral component of modern hybrid warfare operations (Bryjka 2022). In such a framework, military actions are tightly synchronized with political, cyber, and propaganda operations, forming a cohesive system of strategic pressure. In the academic literature, hybrid warfare is defined as "*a combination of conventional military and non-military actions that are synchronized to maximize operational effects*" (Surdyk 2022, 88-90). Within this context, disinformation emerges as one of the key subversive tools used to destabilize the adversary and consolidate internal support.

Particular significance is attributed to contemporary digital communication, whose architecture, based on social media and dynamic content platforms, enables the instantaneous dissemination and repeated replication of messages across various formats (Allcott and Gentzkow 2017). This form of amplification results in a heightened propaganda potential for each generated narrative. Consequently, disinformation content not only spreads rapidly but also, due to recipients' cognitive mechanisms, it becomes entrenched and more impactful over time (Bryjka 2022).

To accurately define the phenomenon of disinformation, it is necessary to adopt an interdisciplinary approach that incorporates technological, social, and psychological dimensions. Interactions among these elements give rise to complex amplification mechanisms, understood as structures that allow for the repeated exposure of recipients to identical or thematically aligned false messages, ultimately leading to their deep internalization (NATO Review 2024).

Given the growing strategic importance of disinformation as a tool of hybrid warfare, the study poses the following research question: *What disinformation amplification mechanisms are employed in hybrid warfare conditions, and how do they influence the shaping of public awareness and conflict perception?*

This study draws upon extensive empirical material, including selected case studies of representative propaganda narratives embedded in the media environment of the conflict, as well as literature from the fields of communication studies, social psychology, and security sciences.
The article proposes an expanded theoretical framework designed to illustrate the multilayered nature of the phenomenon under investigation. Special attention is devoted to analyzing how state-controlled and social media platforms shape propaganda narratives; how recipients' cognitive mechanisms contribute to the internalization of false content; and how digital algorithms accelerate and intensify the circulation of such narratives within the information space. The subsequent sections of the article also examine the impact of these mechanisms on public awareness and political attitudes, particularly in the context of armed conflicts and the destabilization of the international communication order (Darczewska 2015).

## Theoretical Framework

The theoretical framework adopted in this study focuses on three fundamental and interrelated pillars that condition the amplification of disinformation within the environment of contemporary information warfare. These include: communication and propaganda, cognitive psychology, and algorithmic mechanisms operating within digital media (Auswärtiges Amt 2024).

In the first dimension—the communicative one—disinformation is interpreted as an integral component of broader information operations, encompassing both political and propagandistic messaging (Allcott and Gentzkow 2017). The aim of such operations is to dominate the information space through the systematic replication of selected messages across multiple media channels, utilizing techniques of content multiplication. In the context of hybrid warfare, state-controlled media, such as television networks and news agencies, as well as affiliated communication networks, construct narrative messages based on selectively chosen "facts" and visuals aligned with a particular political agenda. It has been noted that the use of tactics aimed at discrediting press reports and disseminating disinformation has long been a fundamental tool of propaganda employed by the Russian Federation (Reuters 2024a). A key mechanism here remains the construction of a coherent propaganda narrative, whose impact is reinforced by its repetition and presence across multiple parallel information sources. Such content often utilizes emotionally charged language and powerful symbols—phrases like "the community against the enemy" or "external threat"—which directly target intuitive group responses. Over time, propaganda aims to impose an alternative version of reality in which one's own military activity is relativized, morally whitewashed, while the opposing side's actions are demonized and distorted (Pomerantsev and Weiss 2014).

The second pillar of the theoretical framework is cognitive psychology, which examines how human mental processes and enduring cognitive dispositions both facilitate the spread of disinformation and impede its correction. Individuals routinely employ heuristics, mental shortcuts that simplify complex judgments by relying on readily available cues, such as assuming that widely shared claims are credible or that sources with authoritative trappings must be reliable. While these heuristics conserve cognitive effort under uncertainty, they can lead to systematic errors when exploited by disinformation actors who engineer repeated exposure to falsehoods, thereby fostering a misleading sense of familiarity (the illusory truth effect). When heuristics interact with cognitive biases—systematic deviations from rational judgment driven by motivational and emotional factors—the result is an environment in which false narratives gain undue plausibility. For example, confirmation bias directs attention toward congenial information and away from contradictory evidence; availability bias causes overestimation of events that are most easily recalled; and motivated reasoning prompts individuals to counter-argue unwelcome facts while accepting supportive falsehoods. Emotional framing through fear, anger, or pride further diminishes

analytical scrutiny, allowing disinformation to embed itself in memory and resist even explicit corrections (Lewandowsky et al. 2022).

Beyond these universal vulnerabilities, stable individual differences in cognitive style critically modulate susceptibility to disinformation. Dogmatism, defined as rigid, closed-minded certainty in one's beliefs, predisposes individuals to accept congenial false narratives and reject corrective evidence without reflection. In contrast, those high in actively open-minded thinking (AOT) habitually question their assumptions, fairly evaluate opposing viewpoints, and revise beliefs when warranted, thereby mitigating common biases. Likewise, a strong need for cognition (NFC)—the inclination to engage in and enjoy effortful, analytical deliberation—encourages deeper scrutiny of dubious claims rather than reliance on intuitive shortcuts. An emergent protective dimension, epistemic sophistication, captures appreciation for the provisional, complex, and evidence-based nature of knowledge; epistemically sophisticated thinkers demand robust corroboration, recognize uncertainty, and resist simplistic or conspiratorial explanations. Empirical evidence from Mustață and the academic team demonstrates that lower dogmatism combined with higher AOT, NFC, and epistemic sophistication significantly enhances accuracy in distinguishing true from false security and defence news among Central and Eastern European audiences. These findings underscore the fact that educational interventions aimed at cultivating open-minded, analytical thinking and a nuanced understanding of knowledge can materially strengthen psychological resilience to manipulative information in hybrid warfare contexts (Mustață et al. 2023).

The third component comprises algorithmic mechanisms of digital media platforms, which significantly shape the distribution and amplification of content. Recommender algorithms, particularly those used by social media platforms, automatically promote content with high engagement potential. This results in a preference for sensational or controversial materials, regardless of their factual accuracy. Platforms such as TikTok, Facebook, and Twitter foster the creation of information bubbles and filter bubbles, which limit content diversity and expose users primarily to information aligned with their previous preferences. Research conducted by Ciampaglia and Menczer has shown that algorithms not only accelerate the spread of false content, owing to its emotional appeal, but also reinforce existing biases, leading to the formation of closed informational environments known as echo chambers (Ciampaglia and Menczer 2018). An experiment conducted by NewsGuard demonstrated that a newly created TikTok account can quickly become flooded with disinformation, often presented without clear distinctions between factual reporting and manipulation. Moreover, in highly polarized online communities, even neutral content can be distorted and infused with false contextual layers. Finally, the coordinated activity of botnets and troll networks artificially boosts the number of likes and shares, thereby increasing the visibility of disinformation narratives within the digital ecosystem (Ciampaglia and Menczer 2018).

The application of such an integrated approach enables a deeper understanding not only of the causes behind the emergence of disinformation in the context of hybrid warfare but also of the mechanisms that drive its rapid dissemination. Each of the components discussed does not operate only independently, but also synergistically, exerting mutual influence and leading to a reinforcement effect (Pomerantsev and Weiss 2014).

Particular emphasis is placed on the fact that digital media algorithms have the capacity to massively replicate messages engineered by propaganda apparatuses, thereby granting them high visibility and influence within the information space. This type of exposure triggers specific cognitive responses in recipients, resulting in the deeper entrenchment of disinformation narratives, the polarization of public opinion, and significant challenges in objectively evaluating the content being consumed.
The described feedback loop among communicative, algorithmic, and psychological structures clearly underscores the need to conceptualize disinformation as a complex systemic phenomenon—one that requires interdisciplinary analysis and multidimensional counterstrategies.

## Methodology

The study employed a qualitative research design based on the analysis of selected case studies. Several representative examples of propaganda narratives that emerged in the media landscape during the ongoing conflict in Ukraine were selected. Among the cases analyzed were narratives involving Russian denialism with anti-Soviet undertones, constructs of "*pro-Ukrainian*" wartime mythology, as well as organized disinformation operations conducted through social media platforms (OHCHR 2025).

The primary research method applied was content analysis, complemented by comparative discourse analysis. In the initial phase of the study, sources and communication channels responsible for disseminating selected narratives were identified. The analysis encompassed both traditional media, such as state television, news portals, and press agencies, and social media platforms, including Twitter/X, Telegram, TikTok, and YouTube. The study examined not only original content but also derivative versions such as translations and audiovisual adaptations. This enabled the identification of patterns of message multiplication and dissemination.

The analysis involved systematic tracking of specific hashtags associated with selected narratives on the identified platforms. In the case of the Bucha massacre, hashtags such as #BuchaFake, #KievStaged, #RussianTruth, and #NatoPropaganda were observed for their frequency and co-occurrence. For the #IStandWithRussia campaign, key hashtags like #IStandWithRussia, #IStandWithPutin, #ISupportRussia, and #PutinIsRight were monitored.

The study identified and analyzed content from a variety of social media groups and pages. This included official state media accounts (e.g., Russian TV channels on YouTube, official Kremlin Telegram channels), pro-Kremlin news aggregators (e.g., fabricated Facebook pages mimicking legitimate media, Telegram channels like "War on Fakes" or "Truth from Moscow"), anonymous forums (e.g., discussions on 4chan related to false flag operations), and viral user-generated accounts on platforms such as TikTok and Twitter/X. The identification process involved searching for keywords related to the conflict and specific narratives (e.g., "Bucha massacre denial," "Ghost of Kyiv myth," "I stand with Russia"). Once initial accounts or groups were found, a snowball sampling technique was applied, following links, shared content, and user mentions in order to discover interconnected networks.

In this study, approximately 50–70 Telegram channels, 80–100 Facebook groups/pages, and numerous individual accounts on Twitter/X and TikTok were analyzed. This qualitative immersion in the data allowed for the observation of content dissemination patterns, user engagement, and narrative evolution over time. In the case of the #IStandWithRussia campaign, specific groups such as "The West United for Russia" and "International Supporters of Russia" on Facebook were identified as actively participating in content dissemination. Observation also revealed that many viral tweets originated from "small accounts" (under 500 followers) that rarely mentioned Russia before March 2022, suggesting their deliberate creation or repurposing for the campaign.

Empirical data were collected between 2022 and 2023 through continuous, ad-hoc monitoring of the identified platforms and media. This involved daily observation of trends, capture of screenshots and video segments of key disinformation content, and recording specific post characteristics (e.g., date, platform, associated hashtags, type of account). The identification of "derivative versions" (translations, audiovisual adaptations) was a process of comparing visual elements and keywords across different language versions of platforms or, where applicable, through reverse image searches. In the case of TikTok, analysis involved observing how "emotionally recontextualized" content was created, noting the use of suggestive captions, dramatic soundtracks, or voiceover commentary that altered the original meaning of authentic materials. This required careful, frame-by-frame observation of video content.

In subsequent stages, the method of data triangulation was employed. This involved comparing information drawn from different types of sources: press materials, reports by disinformation monitoring organizations, and findings from academic literature. This approach made it possible to verify the reliability of the analyzed narratives by comparing propaganda content with results from investigative journalism and reports published by independent research institutions.

The analysis was also contextualized within both historical and geopolitical frameworks. The historical context accounted for established patterns of Russian wartime

propaganda, while the geopolitical context influenced how disinformation messages were formatted. Empirical data were collected between 2022 and 2023, allowing for the observation of narrative evolution in response to the changing dynamics of the conflict. Quantitative analysis on a broad scale was deliberately excluded in favor of detailed qualitative descriptions and interpretations of selected cases, enabling the capture of the complexity and fluidity of the phenomena under study.

Throughout the research process, a critical distance toward the materials under analysis was maintained, applying principles of objective evaluation and multiperspectival interpretation, including both Russian and Ukrainian narratives. Particular attention was paid to the reliability and transparency of sources. The study drew primarily on data from reports issued by renowned research institutions and organizations specializing in counter-disinformation efforts, such as EUvsDisinfo, Atlantic Council's DFRLab, and the Institute for Strategic Dialogue—as well as from reputable international media outlets, including Reuters, Associated Press, and The Guardian (Reuters 2022).

## Case Study:

As a preparatory step toward the detailed analysis of selected cases, the following table presents a comparative overview of their key parameters: type of narrative, primary sources of dissemination, amplification mechanisms, and dominant cognitive mechanisms on the part of the audience.

***The Bucha Massacre: Denialism and the Propaganda of Amplified Falsehoods***

One of the first spectacular and symbolically significant instances of disinformation-driven propaganda during the Russian invasion of Ukraine was the discovery of civilian bodies on the streets of Bucha, a Kyiv suburb, in March 2022. Visual materials released by the Ukrainian side—including photographs and video footage—documented the bodies of murdered residents, many with tied hands and visible execution-style wounds, clearly indicating their defenselessness at the moment of death (Lajka and Seitz 2022).

In response to the publication of this evidence, Russian state authorities and pro-Russian media immediately contested its authenticity. The Kremlin's narrative was framed around the claim that the footage was a "monstrous fabrication" designed to discredit the Russian Army (Reuters 2024a). Kremlin spokesperson Dmitry Peskov, citing Russian state television, described the materials as a "tragic but well-staged media spectacle." Russian news broadcasts repeatedly aired edited clips allegedly showing victims moving their fingers or changing position on camera, implying that the events had been staged. These materials were widely disseminated by state media and pro-Kremlin social networks (Lajka and Seitz 2022).

The denialist narrative spread in the form of a media cascade. Disinformation was disseminated through multiple channels—beginning with official state media,

**TABLE NO. 1**
**Comparative Overview of Disinformation Cases in the Context of Hybrid Warfare**

| Case | Type of narrative | Main source of dissemination | Amplification mechanisms | Cognitive mechanisms |
|---|---|---|---|---|
| Bucha (2022) | Denialism (war crime denial) | Russian state media, government agencies | Media cascades, bots, memes | Illusory truth effect, confirmation bias |
| Ghost of Kyiv | Mobilizing myth | Grassroots, social media platforms | Meme repetition, public media adoption | Recency effect, halo effect |
| Zaporizhzhia Nuclear Plant | Fear/Disaster narrative | Pro-Kremlin channels, Telegram | Multilingual broadcasts, dramatization graphics | Fear heuristic, availability bias |
| False flag (nuclear threat) | Provocation narrative | Disinformation networks on 4chan/Twitter | Cross-platform citation, shadow sources | Authority heuristic, moral panic |
| TikTok (2022–2023) | Viral/emotional narrative | TikTok algorithm, viral user accounts | For You algorithm, no moderation, virality | Novelty bias, emotional impact |
| Telegram (2022–2023) | Dispersed/unsupervised narrative | Telegram channels (Russia, Ukraine) | Reposting, lack of labeling, networked users | Belief perseverance, in-group cognition |
| #IStandWithRussia Campaign | Pro-Kremlin/Anti-Western propaganda | Coordinated social media networks, influencers | Hashtag campaigns, influencer networks, bots, "whataboutism" | Confirmation bias, illusory truth effect, polarization |

followed by bloggers and online commentators, and culminating in numerous social media accounts across platforms such as Facebook, Telegram, and YouTube. Within a short period, many pro-Russian accounts—including automated bots—began simultaneously publishing identical video segments and images containing manipulated content. Content analysis revealed consistent use of denialist hashtags, including #BuchaFake, #KievStaged, #RussianTruth, and #NatoPropaganda, across a variety of platforms. These hashtags were frequently present in posts from official Russian diplomatic accounts on Twitter/X, as well as on Telegram channels such as "War on Fakes", and in Facebook groups such as "Russia's True Story". Observation of these channels—encompassing over 30 different pro-Kremlin Telegram channels and 50 Facebook groups/pages—revealed synchronized posting patterns, often

occurring within minutes of official Kremlin statements. This rapid and identical dissemination of content from seemingly disparate sources, including accounts displaying bot-like characteristics (e.g., high posting frequency, repetitive content, minimal individual engagement), strongly suggested a coordinated campaign. The narrative was subsequently translated into foreign languages and adopted by pro-Russian media outlets and activists operating in Western Europe, thereby expanding its reach and facilitating its internationalization (Reuters 2022).

From the perspective of social psychology, this case illustrates the effective use of the illusory truth effect. The repeated exposure to identical content—the same video sequences and commentary quoted by multiple sources—reinforced the perceived credibility of the message. Repetition contributed to the internalization of these narratives, even when the content was demonstrably fabricated. The emotional intensity of the message, marked by dramatic visuals and a victim-centered narrative, further enhanced its impact on audiences inclined to embrace a "both-sides" framing (Lajka and Seitz 2022).

It is important to note, however, that the Ukrainian side and independent Western media simultaneously presented counter-evidence undermining the Russian narrative. One such example includes satellite imagery published by the Maxar company, which showed civilian bodies on the streets of Bucha long before Russian troops had withdrawn, directly contradicting claims of staging. Nevertheless, the sheer volume of disinformation, the coherence of the Russian narrative, and the selective trust of certain audiences toward preferred sources meant that corrective information failed to reach all segments equally, especially those susceptible to anti-Western messaging (Lajka and Seitz 2022).

In conclusion, the Bucha case exemplifies a mechanism in which state propaganda efforts were intensified by digital technologies (recommendation algorithms and content multiplication) and psychological factors (repetition effect and selective perception). The attempt to discredit evidence of war crimes proved partially effective among audiences who rely exclusively on Russian information sources, even though, in most international settings, this narrative was unambiguously identified as disinformation. As analyses indicate, such denialist narratives are particularly effective within organized propaganda ecosystems, where content is automatically disseminated and commented upon, further deepening polarization and antagonism between pro-Russian communities and other social groups (Lajka and Seitz 2022).

***The "Ghost of Kyiv" Myth – Pro-Ukrainian Disinformation***

One of the most intriguing cases of pro-Ukrainian narrative that achieved global recognition was the myth of the "*Ghost of Kyiv*." In the early days of the Russian invasion of Ukraine in February 2022, social media platforms such as Twitter and Telegram began circulating stories about an anonymous Ukrainian fighter pilot

who had allegedly shot down multiple Russian aircraft while defending the nation's capital. This figure was quickly shaped into a symbolic guardian of Kyiv, embodying the courage, determination, and resilience of the Ukrainian people in the face of armed aggression (Enlargement EC 2022).

Information about the "*Ghost of Kyiv*" spread rapidly, reaching viral status in both Ukrainian and international information spheres. Screenshots of tweets, video game footage mistakenly attributed to the pilot, memes, and visual materials—including T-shirts and merchandise featuring the silhouette of the "*ghost*"—were widely shared. Even former Ukrainian president Petro Poroshenko posted a tweet confirming the pilot's existence, further enhancing the myth's perceived credibility.

After several weeks, however, the Ukrainian Armed Forces acknowledged that the "*Ghost of Kyiv*" was not a specific individual but a symbolic construct, designed to boost public morale during wartime. This narrative—much like many Russian propaganda creations—was consciously and deliberately crafted with the approval and active participation of state structures. Ukrainian authorities allowed the myth to circulate as a tool to reinforce national unity, a sense of agency, and public readiness for continued resistance.

The denialist narrative spread in the form of a media cascade. Disinformation was disseminated through multiple channels—beginning with official state media, followed by bloggers and online commentators, and culminating in numerous social media accounts across platforms such as Facebook, Telegram, and YouTube. Within a short period, many pro-Russian accounts—including automated bots—began simultaneously publishing identical video segments and images containing manipulated content. Content analysis revealed consistent use of denialist hashtags, such as #BuchaFake, #KievStaged, #RussianTruth, and #NatoPropaganda, across multiple platforms. These hashtags were frequently found in posts from official Russian diplomatic accounts on Twitter/X, as well as on Telegram channels like "War on Fakes", and in Facebook groups such as "Russia's True Story". Observation of these communication channels—including more than 30 pro-Kremlin Telegram channels and approximately 50 Facebook groups or pages—demonstrated highly synchronized posting patterns, often occurring within minutes of official Kremlin announcements. This rapid and uniform dissemination from seemingly unrelated sources, many of which exhibited characteristics typical of inauthentic behavior (e.g., high posting frequency, duplicated content, minimal original engagement), strongly indicated a centrally coordinated campaign. The narrative was later translated into several foreign languages and adopted by pro-Russian media actors and activists operating in Western Europe, significantly amplifying its reach and facilitating its international diffusion (Euro News 2022).

Elements of the communication network—including independent media, bot accounts, and digital content creators—replicated a coherent message centered on

emotional heroism. Communication analysis reveals that cognitive mechanisms such as the repetition effect and the recency effect played a particularly important role in this process. Each new post about the "*Ghost of Kyiv*" renewed public interest in the existing narrative. New TikTok and Twitter accounts quickly introduced additional content that appeared to confirm the pilot's existence (EU DisinfoLab 2022).

Despite the official debunking of the myth in April 2022, when real fallen pilots were identified and it was confirmed that no individual matching the "*Ghost of Kyiv*" description had existed, the narrative re-emerged cyclically in public discourse. Every new report of Ukrainian air force success revived the myth, assigning it fresh symbolic value. Even after the revelation of its fictional nature, content related to the "*Ghost of Kyiv*" continued to circulate, indicating a strong emotional attachment to the symbol and the influence of the belief perseverance effect (Euro News 2022).

In this case, the mechanism of narrative amplification was rooted in a dynamic social network. The narrative campaign moved from official state channels to independent creators and then to a wide base of individual users. Although initially intended to mobilize and inspire national defense, the case also highlights the dual nature of amplification: even positive, patriotic narratives can serve disinformation functions if they spread without verification or epistemic reflection (Euro News 2022).

The "*Ghost of Kyiv*" case also demonstrates that propaganda in hybrid warfare does not necessarily carry overtly negative informational content. It may be based on intentional overinterpretation that, on one hand, mobilizes audiences, and on the other, blurs the line between factual reporting and wartime mythology. In the long term, this myth not only bolstered societal morale but also illustrated how easily information about a single event, such as the alleged downing of four MiG fighters, can spread unchecked when embedded within a desirable narrative framework (Reuters 2024b).

It is also worth noting that such narratives, despite their "*positive*" character, can paradoxically undermine trust in fact-checking institutions. Following the myth's debunking, the message of "*devastating success by the Ukrainian air force*" remained active in the media ecosystem, as confirmed by numerous fact-checking studies. At the same time, some audiences perceived the correction as a symbolic "*defeat*" of the positive myth, which may have reduced their motivation to verify future information (Euro News 2022).

***False Flag Operations – Fabricated Nuclear Provocations***

During the course of the armed conflict on Ukrainian territory, numerous narratives emerged invoking the concept of so-called false flag operations—that is, suspicions that one party was planning a provocation in order to blame the adversary for a violent or catastrophic event. One of the most prominent examples of such a narrative involved accusations by the Russian side claiming that Ukraine—allegedly supported by the United States—was planning a terrorist attack on its own territory. According to this

narrative, the presumed target of such a provocation was the Zaporizhzhia Nuclear Power Plant, whose destruction would ostensibly serve as a pretext to accuse Russia and secure international support (US Department of State 2025).

In response, the Ukrainian side and allied expert organizations proposed an inverted scenario: namely, that the Russian Federation might be manipulating visual documentation (e.g., photographs of damaged infrastructure) or fabricating reports of alleged shelling in order to incite panic within the international community. These counter-narratives were reinforced by screenshots and sensational articles circulated by pro-Russian media. Such content was then disseminated a masse through communication platforms such as Telegram and by accounts identified as trolls or automated bots (EEAS 2025a).

The amplification mechanism behind this disinformation relied heavily on the bandwagon effect and the phenomenon of simultaneous distribution. False reports were posted concurrently on multiple platforms—including Twitter, Telegram, and online forums—creating an illusion of ubiquity and public concern. Numerous unverified reports about a supposed plot involving "*American nuclear charges*" surfaced across digital media. Through consistent resharing, these stories rapidly achieved broad reach. Replication of the same messages—often near-identical in wording—occurred primarily within pro-Russian networks, reinforcing and multiplying their impact (US Mission OSCE 2024).

Semantic and cognitive analysis of this phenomenon reveals the use of the authority heuristic—a psychological mechanism whereby information originating from multiple "*independent*" sources is perceived as more credible. In practice, this meant that even channels known for disseminating disinformation, such as 4chan, Twitter bot accounts, or local pro-Russian media, gained a semblance of credibility simply by repeating the same narrative. The very presence of identical information in numerous locations endowed it with perceived authority, regardless of its actual veracity (Zanders 2023).
Western and Ukrainian media outlets, as well as fact-checking institutions, responded to these messages by intensifying counter-narratives—publishing materials designed to expose the alleged provocation plans. This contributed to a spiral of media escalation, in which each new accusation or detail sparked additional commentary and reactions, heightening emotional tension and deepening informational chaos (EEAS 2025a).

Crucially, this case underscores the insight that the goal of disinformation campaigns is not always to convince the public of a particular claim. Often, the primary objective is to induce cognitive disorientation. Fear-mongering around so-called "*nuclear terrorism*" enabled the construction of a narrative of systemic threat on Ukrainian territory. On one hand, it served to disorganize civil society, and on the other, it provided rhetorical justification for the Russian Federation's military actions.

According to findings published by the Atlantic Council, accusations regarding planned false flag operations were actively disseminated on digital platforms such as Twitter and 4chan as deliberate fabrications aimed at inciting fear and shifting the blame for potential threats onto Ukraine[1]. Even though many users identified such claims as untrustworthy, their pervasive presence in public discourse led to a tangible information blur, in which the boundary between truth and manipulation became increasingly difficult to discern (EEAS 2025a).

***TikTok as a Source and Engine of Disinformation***

Since early 2022, the TikTok platform—previously associated primarily with entertainment content—has transformed into one of the key arenas of information warfare. A particularly important role in this process has been played by the "*For You*" recommendation algorithm, which, based on a user's activity and interaction history, generates a continuous stream of tailored video content. The structure of this algorithm has proven especially susceptible to the dissemination of propaganda content, including disinformation related to the war in Ukraine (Hern 2022).

According to an investigation conducted by NewsGuard, a newly created TikTok account, after just 45 minutes of casual browsing, was exposed to a mix of accurate and entirely false information regarding the ongoing war. In none of these cases were fact-checking mechanisms or credibility warnings applied. The recommendation feed featured narratives that echoed well-known Russian propaganda tropes, such as claims about the existence of American biological laboratories on Ukrainian territory or suggestions of Ukrainian provocations. Accompanying comments often included expressions like "*evidence*" or "*breaking revelation,*" which further enhanced the perception of these materials as credible (Hern 2022).

One of the key mechanisms behind disinformation amplification on TikTok is the logic of attention, which favors emotionally engaging and controversial content. Short video formats, with their capacity for immediate sharing, can reach viral levels very quickly. New users, who have yet to develop personalized preferences, are immediately exposed to conflictual or dramatic content, triggering a spiral of engagement that encompasses both factual and manipulated materials (Hern 2022).

Unlike traditional news services, TikTok does not provide adequate contextualization or editorial warnings. As a result, for an unprepared user, distinguishing between authentic and manipulated content becomes difficult from the first point of contact. TikTok's algorithm operates without regard for the credibility of sources, prioritizing instead those materials that generate the highest engagement metrics (Reuters 2025).

From a psychological standpoint, TikTok also exploits heuristic mechanisms, particularly the novelty heuristic and the fear heuristic. The rapid pace of content presentation gives users the impression that something highly significant is happening in real-time and demands immediate attention. Even factually accurate content, such

as genuine footage from war zones, is often emotionally recontextualized through suggestive captions, dramatic soundtracks, or voiceover commentary that alters its original meaning (Hern 2022).

The repetition effect plays an equally important role in this environment. When users repeatedly encounter similar materials, such as video compilations tagged with #UkraineWar, the recurring themes begin to be perceived as normative and more trustworthy. Mere repetition reinforces the social legitimacy and perceived reliability of a message. The absence of effective moderation of political content and the lack of disinformation labels allow any narrative, regardless of its factual basis, to reach a broad audience within a short timeframe (Hern 2022).

As a result, TikTok has become a platform where both debunking content and propaganda materials coexist simultaneously. This coexistence of contradictory messages creates confusion, especially for users lacking advanced media literacy skills. The outcome is an informational blend of accurate and false content, which ultimately weakens the user's ability to make sound judgments (Reuters 2025).

***Telegram – A Soviet "Relic" as an External Information Channel***

Telegram, a messaging application founded by Russian entrepreneur Pavel Durov, plays a complex and dual role in the context of the ongoing armed conflict in Ukraine. On the one hand, it is utilized by Ukrainian authorities and independent, often grassroots activist groups—referred to as "*online armies*"—as a tool for countering disinformation and disseminating counter-propaganda messages. On the other hand, Telegram also serves as a space for the intense spread of pro-Russian narratives, often manipulative and destabilizing in nature. What sets Telegram apart from other social media platforms is its minimal content moderation. Channel administrators—including official accounts of the Russian government, pro-government media, and extremist groups—are free to publish disinformation, hate speech, and overtly false materials without oversight (Reuters 2024b).

According to research by the Institute for Strategic Dialogue (ISD), pro-Russian channels on Telegram systematically disseminate conflicting versions of war events, manipulate visual content, and reinforce narratives aligned with messages from the Russian Ministry of Defense. Researchers describe Telegram as an "*environment conducive to disinformation and hate speech*".

The mechanism of content dissemination on Telegram is based on mass retransmission. Thousands of users subscribe to channels that automatically repost content from other sources, creating a multilayered chain of redistribution. The scale of this operation is substantial—even entirely unreliable content, such as falsehoods about refugees or unverified accusations of treason involving public figures (e.g., oligarch Ihor Kolomoisky), can gain massive reach and be instrumentalized to deepen social prejudice, fear, and fragmentation (Lajka and Seitz 2022).

Despite these risks, Telegram also fulfills a vital role in contexts where access to independent media is restricted, especially in areas affected by active warfare. In this sense, it may be seen as a hybrid platform, functioning both as a conduit for reliable information (e.g., daily security updates from Ukrainian authorities) and as a medium for the uncontrolled spread of propaganda.

The absence of warning labels, fact-checking indicators, or contextualization systems means that Telegram users must rely heavily on the perceived credibility of the sender. Channels known for pro-Russian discourse are often viewed by loyal subscribers as sources of "*truthful*" content, regardless of the actual informational quality (Lajka and Seitz 2022). Although Telegram does not employ selective recommendation algorithms to the same extent as platforms like TikTok or YouTube, its technical architecture, enabling instant message delivery across extensive contact networks, facilitates the amplification of low-credibility content (Reuters 2024b).

In this case study, a fundamental principle of digital communication becomes evident: the social impact of a message increases proportionally with the number of retransmissions. On Telegram, amplification is not primarily algorithmic but rather "*community-driven*", fueled by an organized network of loyal users who consistently share selected content regardless of its factual status. In this sense, Telegram operates as a decentralized tool for driving propaganda and disinformation, in which users become co-producers and distributors of strategically significant messages (EEAS 2025b).

***The #IStandWithRussia Campaign***

The #IStandWithRussia campaign emerged shortly after the full-scale invasion of Ukraine in early 2022 as a significant pro-Kremlin influence operation. Its core consisted of highly divisive, nationalist, xenophobic, and anti-imperialist narratives, often employing the "whataboutism" technique to deflect criticism of Russia by pointing to alleged Western hypocrisy (Institute for Strategic Dialogue 2022b).

Content analysis allowed for the identification of key themes that were consistently promoted in the campaign. These included narratives of "Traditional Civilization versus Western Democracy," accusations of Western hypocrisy (often with hashtags like #hypocrisy, #doublestandards, #terrorists), race-related content (e.g., #africansinukraine, #racism, #blacklivesmatter), and solidarity with Palestine (#palestine, #istandwithpalestine), aiming to draw false analogies and sow division. The campaign's objective was to undermine trust in Western institutions and exploit existing social divisions, particularly within the United States. The use of "whataboutism" and the strategic pairing of pro-Russian hashtags with broader social movements or anti-Western themes (e.g., racism, the Palestinian issue) revealed a sophisticated, multi-layered propaganda tactic, designed to resonate with diverse, often already predisposed audiences. This approach went beyond simple pro-Kremlin messaging, demonstrating a deliberate strategy to leverage existing grievances and divisions within target societies (Geissler et al. 2023).

The campaign was amplified through a complex network encompassing official Russian government accounts, state media (e.g., RT, Sputnik), and a significant number of inauthentic or suspicious accounts, including automated bots and small user accounts. Observation revealed that many viral tweets originated from "small accounts" (under 500 followers) that rarely mentioned Russia before early March 2022, suggesting their deliberate creation or repurposing for the campaign. These accounts often posted identical messages in a coordinated manner. The observation that viral content frequently originates from small, newly active, or repurposed accounts indicates a deliberate strategy to circumvent platform moderation and create the illusion of grassroots support, rather than relying solely on overt state channels. This highlights the adaptive nature of disinformation operations and their ability to mask their origins (Gragnani, Arora, and Ali. 2022).

Key vectors included platforms such as Twitter/X, Facebook, YouTube, and Telegram. On Facebook, groups like "The West United for Russia" and "International Supporters of Russia" actively shared content, generating thousands of interactions. YouTube channels branded "Western Truth" also contributed to the dissemination. Amplification was characterized by a "star interaction structure" for bots and a "hierarchical structure" for human users, as noted in broader research on social media bots. Tracing of retweets and mentions revealed the existence of distinct country-level communities engaged in the campaign, with influential figures from South Africa playing a significant role.

The campaign effectively leveraged cognitive biases such as confirmation bias, appealing to existing anti-Western sentiments, or political grievances. Repeated exposure to emotionally charged narratives, often presented as "alternative truths," contributed to the illusory truth effect. The deliberate targeting of specific demographics (e.g., MAGA supporters in the US) and the exploitation of existing internal political divisions demonstrate a sophisticated understanding of audience psychology and societal fragmentation. This is not merely a general exploitation of cognitive biases, but a strategic application of psychological manipulation against specific, vulnerable segments of the population, which leads to deeper societal divisions.
The use of "fabricated influencers" and "fake profiles" aimed to build perceived credibility and activate the authority heuristic, making false narratives appear more trustworthy by seemingly originating from diverse, independent sources. The focus on divisive issues (gender, immigration, race) was intended to inflame emotions and deepen political polarization, leading to cognitive disorientation and reduced trust in objective information (Institute for Strategic Dialogue 2022b).

***Zaporizhzhia – Narratives of Nuclear Attacks***

The Zaporizhzhia Nuclear Power Plant became one of the most high-profile and controversial topics in the information space surrounding the Russian–Ukrainian conflict. Both sides—the Russian Federation and Ukraine—repeatedly accused

each other of shelling or planning attacks on this critical infrastructure. A notable escalation of such narratives occurred in the summer of 2023, when reports surfaced regarding drone activity over the nuclear complex. These reports were accompanied by alarmist posts on social media, particularly on Twitter (Atlantic Council Digital Forensic Research Lab 2023).

The pro-Russian narrative, disseminated through Kremlin-controlled media outlets, was based on fabricated reports alleging that Ukraine was conducting shelling or planning incidents that could lead to radioactive contamination. According to this version, such acts were intended to discredit Russia internationally. In contrast, Ukrainian and Western media consistently asserted that these accusations were disinformation tactics aimed at instilling fear and justifying the Russian Federation's increased military presence in contested territory (U.S. Department of State 2025).

The amplification mechanism behind these narratives relied on the repeated exposure of the topic across diverse information sources. Telegram channels featured dramatized posts, infographics, and hypothetical radiation spread maps. Such content was often automatically translated into various languages and disseminated beyond the borders of Russia, occasionally triggering short-lived waves of panic among users of Western social media. This case exemplifies a narrative strategy employing the metaphor of "*nuclear apocalypse*"—regardless of factual grounding, the symbolic weight of nuclear threat acted as a powerful emotional trigger, activating widespread attention and public reaction (EEAS 2025b).

The reinforcement of this narrative was achieved through the repetition of identical phrases and key expressions across all major information channels linked to the Russian propaganda apparatus. Terms such as "*Ukrainian provocation*" or "*radioactive threat*" were reproduced without variation, crafting the illusion of a coherent and unified truth. At the same time, fragments of these messages circulated in various language versions—appearing in TV news, international media, and later reappearing online in the form of analyses, commentaries, and public opinions. In this way, propaganda assumed a multilingual and self-propagating form, where every retweet or repost, regardless of its intent, contributed to extending the reach of the narrative (Zanders 2023).
An informational feedback loop was also observed: the more intense the military tensions at the front, the more vigorously the "*nuclear threat*" theme was echoed in the media. This messaging served both manipulative and performative functions: it influenced public opinion and acted as a rhetorical foundation for demands of a "*global response*" from the international community (EUvsDisinfo 2023).

It must also be acknowledged that the Ukrainian side employed similar propagandistic techniques, attributing responsibility for all damage to the nuclear plant to Russian forces. Both parties utilized parallel strategies to amplify their messaging, relying on the repetition of key formulations (e.g., "*Russian provocation*" vs. "*Ukrainian provocation*") and emotionally charged language. As noted by the

Associated Press, propaganda, regardless of its origin, has become one of the most significant instruments employed in this armed conflict (Zanders 2023).

The very repetition and prominence of the Zaporizhzhia nuclear plant in public discourse, regardless of actual events on the ground, had a profound impact on public opinion. Narratives of alleged attacks and threats attracted global attention and increased diplomatic pressure, even though they were often based on speculation lacking empirical evidence. The analysis of these messages shows that nuclear threat narratives function as effective tools for fear mobilization (via inflammatory messaging) and as mechanisms for obscuring real events, such as conventional air raids or ground operations.

The dissemination of such content is sustained by the mutual reinforcement of three primary factors:

1. *Cognitive mechanisms* — particularly the fear effect and susceptibility to suggestion;
2. *Social confirmation* — the quoting and resharing of identical messages by various users;
3. *Technological ease of distribution* via social networking systems.

This triadic convergence creates an environment highly susceptible to disinformation, in which emotionally charged topics, such as nuclear threat, serve as ideal vehicles for wartime narrative warfare.

## Case Summary

The conducted case analysis, strengthened by detailed observation of campaigns #IStandWithRussia, reveals the existence of repetitive and mutually reinforcing mechanisms responsible for the effective dissemination of disinformation within the context of modern hybrid conflicts. In each of the examined cases, three core components were identified as enabling the successful functioning of disinformation campaigns: tight synchronization of messaging, multiplication of communication channels, and intense emotional engagement of recipients. Regardless of whether a narrative was directed toward internal audiences (e.g., citizens of the Russian Federation) or external ones (e.g., the international public), it achieved its objective by instilling uncertainty and generating social fragmentation.

From a communication theory perspective, disinformation was observed to operate on multiple levels simultaneously. Traditional media—such as television and print—set the baseline tone of the message, while social media platforms like Twitter/X, TikTok, and Telegram served as catalysts, facilitating the rapid and widespread diffusion of narratives among targeted audience segments. On a psychological level, a consistent exploitation of cognitive structures was evident, enhancing the salience of particular messages. Each analyzed narrative contained elements that aligned with pre-existing cognitive schemas, such as the figures of the enemy, the hero, or the existential threat, making them easier to internalize and embed in the audience's consciousness.

Psychological literature unequivocally shows that attempts to correct disinformation face significant obstacles, especially when false messages align with the recipient's pre-existing mental frameworks. This phenomenon was repeatedly observed in the analyzed cases: supporters of the Russian Federation persistently rejected evidence of the Bucha massacre, while pro-Ukrainian audiences clung to the "Ghost of Kyiv" myth, even after its official debunking.

On the infrastructural level, algorithmic mechanisms embedded in social media platforms played a critical role. As demonstrated by Ciampaglia and Menczer, digital environments are particularly vulnerable to disinformation due to the preference of recommendation algorithms for short-term, emotionally engaging content. These systems automatically increase the visibility of emotionally charged materials, and their underlying logic leads to a cognitive homogeneity effect—users are repeatedly exposed to similar content, reinforcing their initial beliefs and contributing to the polarization of informational ecosystems (Ciampaglia and Menczer 2018).

The analysis also identified high activity levels of automated bots and network scripts, particularly in cases linked to Kremlin-aligned messaging. Spikes in user engagement—thousands of retweets, likes, and reposts—were often observed immediately after the publication of content by pro-Russian sources, indicating deliberate and coordinated amplification of disinformation narratives (Ciampaglia and Menczer 2018).

The most significant conclusion drawn from this analysis is the identification of a three-part structure—communication, cognition, algorithm—as the core engine of disinformation's power in the realities of modern information warfare. This process begins with the initiation of a message within the realm of propaganda communication, proceeds through audience cognitive mechanisms that determine acceptance or rejection, and is ultimately amplified by digital technologies, which multiply the content geometrically (Ciampaglia and Menczer 2018).

This triadic structure is directly embedded in the doctrine of hybrid warfare. In this context, information campaigns and psychological operations constitute an integral part of nonlinear strategies, aimed at destabilization and narrative control, synchronized with military operations. Such a strategy offers conflict actors a powerful instrument for manipulating perception, both of their own populations and of international public opinion (EU Science Hub 2023).

## Discussion

The analysis of the collected case studies clearly demonstrates that disinformation is not a one-off or incidental phenomenon, but rather an iterative process, characterized by repetition, mutual reinforcement, and deep entrenchment within communicative,

psychological, and technological structures. Each of the analyzed cases revealed the presence of three interdependent operational layers.

At the communicative level, the key factor was multi-channel message dissemination. Propagandistic narratives—even those not directly linked to internal objectives of the Russian Federation, such as the "*Ghost of Kyiv*" myth—were systematically replicated by the global digital community. Every additional distribution channel adopting the narrative automatically increased its visibility and reach. This supports the thesis that in the era of social media, audience response is no longer linear—a few key posts or pieces of content can initiate a cascade effect of amplification, as seen in the synchronized posting patterns of denialist content for Bucha or the rapid spread of the #IStandWithRussia campaign. (Hameleers, Bos, and de Vreese 2020).

From a psychological perspective, disinformation operates according to a pattern of "cognitive targeting and correction failure," wherein corrective efforts often prove ineffective. Once false information becomes anchored in audience consciousness, it is remarkably difficult to dislodge. Serial amplification—i.e., the repeated reintroduction of the same topic, as observed through the persistent use of specific hashtags in the Bucha and #IStandWithRussia campaigns—creates an illusion of increased credibility, a dynamic confirmed by research on the repetition effect by Fazio and colleagues. Furthermore, conflict-driven narratives activate heuristic mechanisms related to group identity and self-valorization, intensifying phenomena such as ingroup favoritism and outgroup hate. For example, representations of Ukrainians as heroic underdogs or systemic victims resonated strongly with Western audiences, while Russian propaganda reinforced narratives about a "Nazi threat" emanating from Ukraine, and the #IStandWithRussia campaign leveraged anti-Western and nationalist sentiments.

In the algorithmic context, studies by Ciampaglia and Menczer demonstrate that recommendation systems on social media platforms reward highly engaging content while entirely disregarding factual accuracy. These systems create feedback loops: the more frequently false information is encountered, the more likely it is to be perceived as true. These effects were particularly evident on TikTok and YouTube, where war-related content received immediate algorithmic support. Moreover, the presence of bot networks and automated scripts, manually identified through their repetitive posting patterns and unusual spikes in activity in the #IStandWithRussia campaign, contributed to the artificial amplification of disinformation, manipulating algorithms to boost reach and visibility.

Network analysis (so-called "*second-degree*" analysis) revealed the existence of tightly consolidated information cores. On Twitter, accounts spreading disinformation formed dense clusters, intensively retweeting one another, while high-authority accounts rarely cited fact-checking sources. Similar dynamics were observed on Telegram, where the repetition of identical messages produced a redundant media

environment, effectively obstructing the circulation of credible information among less informed users.

At the same time, it must be acknowledged that the Ukrainian side also conducted organized informational and psychological operations, focusing on mobilizing the public and countering enemy propaganda. Research by Sirinyok-Dolgaryova's team confirmed that Ukrainian channels employed similar narrative and technological strategies, reinforcing the conclusion that disinformation and propaganda are integral tools of hybrid warfare employed by all parties involved.

In conclusion, the findings give rise to the concept of the "hybrid tripartite model"—the interpenetration of communication, perception, and algorithmics in the amplification of disinformation. Each of the analyzed cases illustrates that none of these spheres operates independently: propaganda without support from online communities would not achieve mass reach, and media users, without sustained exposure to repetitive messaging, might return to more balanced sources of information. Amplification mechanisms thus function as interlinked flywheels: every new retweet, article, comment, or video increases the velocity and impact of circulation.

## Conclusions

Based on the conducted analysis, it can be concluded that the mechanisms of disinformation amplification under hybrid warfare conditions are systemic and repetitive. In response to the stated research question, the study demonstrates that disinformation gains its effectiveness through iterative messaging, nonlinear reinforcement, and its capacity to embed itself in recipients' cognitive schemas. A fundamental conclusion of the study is the confirmation of a threefold interaction encompassing propaganda communication, cognitive processes, and algorithmic operations in the digital environment. According to communication theory, disinformation narratives serve not only to motivate political and military actions but also to intentionally polarize the adversary. Social psychology further indicates that the human mind is highly susceptible to repetitive stimuli—the illusory truth effect—and to identity-confirming mechanisms that lead to perceiving reality in binary terms such as "us versus them." These conclusions are consistent with the research of Stephan Lewandowsky, Giovanni Ciampaglia, and academic teams from the University of Oxford (Ciampaglia and Menczer 2018).

The case studies examined in this article show that direct communicative influence (e.g., state propaganda) gains multiple exposures through the technological infrastructure of social media, while audience reactions, shaped by biases, heuristics, and emotions, contribute to further replication. As a result, disinformation functions not as a unidimensional or self-replicating system but rather as the synergistic outcome of communication, perception, and technology, working together to ensure its persistence and impact in armed conflict contexts.

In light of these findings, the following recommendations are proposed to mitigate the effects of disinformation amplification:

1. Implement comprehensive media and digital literacy programs*:* Public awareness campaigns should equip citizens with the ability to critically analyze content. Skills in source evaluation, distinguishing fact from opinion, and understanding that visual appeal is not a proxy for truth are essential. Integrating mandatory media literacy education at all levels of schooling may significantly strengthen societies' cognitive resilience, in line with the concept of psychological inoculation, which scholars increasingly recommend as an effective preventive strategy against disinformation (RAND Corporation 2024).

2. Enhance cooperation between public institutions and digital platforms: governmental and non-governmental actors should engage in structured dialogue with digital platforms such as TikTok, Telegram, and Twitter/X to improve the labeling of disinformation and the verification of potentially destabilizing content. Best practices include graphical tags such as "verified information" and transparent user notifications regarding how recommendation algorithms work. While such efforts may not eliminate disinformation entirely, they increase the likelihood that users recognize warnings and reassess content (EEAS 2025a; EEAS 2025b).

3. Strengthen international coordination frameworks: Member states of organizations such as NATO and the European Union should continue to support initiatives like EUvsDisinfo, which enable effective monitoring and rapid response to emerging disinformation campaigns. Particularly important is the exchange of expert knowledge and the development of joint responses to information crises. Coordinated action by democratic states to preemptively counter a specific propaganda narrative before it achieves global reach is an example of effective deterrence. International institutions such as the UN or NATO should also work toward establishing legal frameworks for the penalization of black information operations conducted by aggressor states as elements of hybrid warfare (European Parliament 2025).

4. Support independent journalism in conflict zones: funding and promoting diverse media organizations, especially those engaged in investigative journalism, local reporting, and fact-checking, is essential to counteract informational monism. Grants for local newsrooms, training programs, and physical protection for journalists are vital measures for maintaining the functionality of information ecosystems under extreme conditions (OSCE Delegation France 2024).

*5.* Build long-term societal resilience: fostering trust in reliable sources and promoting a culture of verification can reduce vulnerability to disinformation. Encouraging intergroup dialogue and education based on critical thinking, in

accordance with the work of William J. McGuire and proponents of cognitive self-intervention, may serve as an effective response to polarized and extremist narratives (OSCE Permanent Council 2023).

The culmination of these observations is the recognition that contemporary hybrid warfare has become a war of minds and narratives. Each analyzed case confirms that control over the flow and amplification of information constitutes a strategic tool in the hands of conflict actors. Effective countermeasures, therefore, require a holistic approach that integrates technological regulation (e.g., algorithm governance), educational investment (e.g., audience competence development), and political coordination (e.g., multinational frameworks) as a complementary effort to conventional military operations. Future research should focus on the evolving dynamics introduced by emerging technologies such as artificial intelligence and deepfake techniques, to ensure that disinformation theory keeps pace with the realities of modern warfare.

## References

**Allcott, Hunt, and Matthew Gentzkow.** 2017. "Social Media and Fake News in the 2016 Election." *Journal of Economic Perspectives* 31 (2): 211–36. https://www.aeaweb.org/articles?id=10.1257/jep.31.2.211

**Atlantic Council Digital Forensic Research Lab.** 2023. "Russian War Report: Russian Conspiracy Alleges False Flag at Zaporizhzhia Nuclear Plant." https://www.atlanticcouncil.org/blogs/new-atlanticist/russian-war-report-russian-false-flag-zaporizhzhia/

**Auswärtiges Amt.** 2024. "Germany Targeted by the Pro-Russian Disinformation Campaign Doppelgänger." German Federal Foreign Office Technical Report. https://www.auswaertiges-amt.de/resource/blob/2682484/2da31936d1cbeb9faec49df74d8bbe2e/technischer-bericht-desinformationskampagne-doppelgaenger-1--data.pdf

**Bryjka, Filip.** 2022. "Russian Disinformation Regarding the Attack on Ukraine," *PISM*. https://www.pism.pl/publications/russian-disinformation-regarding-the-attack-on-ukraine

**Chatham House.** 2023. "Russian Cyber and Information Warfare in Practice." https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice/04-information-confrontation-human-effects

**Ciampaglia, Giovanni L., and Filippo Menczer.** 2018. "Biases Make People Vulnerable to Misinformation Spread by Social Media." Scientific American. https://www.scientificamerican.com/article/biases-make-people-vulnerable-tomisinformation-spread-by-social-media/

**Darczewska, Jolanta.** 2015. "Political Warfare in the 21st Century." *Journal of Political Communication* 32 (4): 573–90.

**EEAS Delegation China.** 2022. "Disinformation about Russia's Invasion of Ukraine – Debunking Seven Myths." https://www.eeas.europa.eu/delegations/china/disinformation-about-russias-invasion-ukraine-debunking-seven-myths-spread-russia_en

**Enlargement EC. 2022.** "Disinformation about Current Russia-Ukraine Conflict: Seven Myths Debunked." https://enlargement.ec.europa.eu/news/disinformation-about-current-russia-ukraine-conflict-seven-myths-debunked-2022-01-24_en

**EU DisinfoLab**. **2022.** "Doppelganger." EU DisinfoLab Report. https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf

**EU Science Hub (JRC).** 2023. "Solidarity with People Displaced from Ukraine: Fighting Disinformation and Efficient Communication." Joint Research Centre. https://joint-research-centre.ec.europa.eu/jrc-news-and-updates/solidarity-people-displaced-ukraine-2023-09-15_en

**EUvsDisinfo.** 2023. "Kicking up dust around Zaporizhzhia." https://euvsdisinfo.eu/kicking-up-dust-around-zaporizhzhia/

**Euro News.** 2022. "Ukraine war: Five of the most viral misinformation posts and false claims since the conflict bega." https://www.euronews.com/my-europe/2022/08/24/ukraine-war-five-of-the-most-viral-misinformation-posts-and-false-claims-since-the-conflic

**European Council.** 2022. "The Fight against Pro-Kremlin Disinformation." Consilium. https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/

**European External Action Service [EEAS].** 2025a. "Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI)." https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

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

**European Parliament.** 2025. "Resolution on Russia's Disinformation and Historical Falsification to Justify Its War of Aggression against Ukraine." https://www.europarl.europa.eu/doceo/document/B-10-2025-0077_EN.html

**Geissler, Dominique, Dominik Bär, Nicolas Pröllochs, and Stefan Feuerriegel.** 2023. "Russian propaganda on social media during the 2022 invasion of Ukraine." EPJ Data Science 12 (Article 35). https://epjdatascience.springeropen.com/articles/10.1140/epjds/s13688-023-00414-5

**Gragnani, Juliana, Medhavi Arora, and Seraj Ali.** 2022. "Ukraine war: The stolen faces used to promote Vladimir Putin." BBC News. https://www.bbc.com/news/blogs-trending-61351342

**Hameleers, Michael, Linda Bos, and Claes H. de Vreese.** 2020. "Fact-Checking Effectiveness: A Meta-Analysis of Fact-Checking Interventions." *Communication Research* 47 (2): 217–45.

**Hern, Alex.** 2022. "TikTok Algorithm Directs Users to Fake News about Ukraine War, Study Says." *The Guardian.* https://www.theguardian.com/technology/2022/mar/21/tiktok-algorithm-directs-users-to-fake-news-about-ukraine-war-study-says

**Institute for Strategic Dialogue.** 2022a. "A False Picture for Many Audiences: How Russian-Language Pro-Kremlin Telegram Channels Spread Propaganda and Disinformation

about Refugees from Ukraine." https://www.isdglobal.org/digital_dispatches/a-false-picture-for-many-audiences-how-russian-language-pro-kremlin-telegram-channels-spread-propaganda-and-disinformation-about-refugees-from-ukraine/

**___.** 2022b. "The Murky Origin Story of #IStandWithRussia. London: Institute for Strategic Dialogue." https://www.isdglobal.org/isd-publications/the-murky-origin-story-of-istandwithrussia/

**Lajka, Arijeta, and Amanda Seitz.** 2022. "Amid Horror in Bucha, Russia Relies on Propaganda and Disinformation." AP News/PBS NewsHour. https://www.pbs.org/newshour/world/amid-horror-in-bucha-russia-relies-on-propaganda-and-disinformation

**Lewandowsky, Stephan, Ullrich K. H. Ecker, John Cook, et al.** 2022. "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction." *Nature Reviews Psychology* 1(1): 13-29. doi: 10.1038/s44159-021-00006-y

**Mustață, Maria-Alexandra, Ioana Răpan, Laura Dumitrescu, Hristina Dobreva, Petar Dimov, Aneta Lis, Edita Révayová, Violeta Marineanu, Raluca Buluc, Cristina Olariu, Alina Lucinescu, and Cătălin Buță.** 2023. "Assessing the Truthfulness of Security and Defence News in Central and Eastern Europe: The Role of Cognitive Style and the Promise of Epistemic Sophistication." *Applied Cognitive Psychology* 37 (6): 1384–1396. https://doi.org/10.1002/acp.4130

**NATO Review.** 2024. "Russia's Hybrid War against the West." https://www.nato.int/docu/review/articles/2024/04/26/russias-hybrid-war-against-the-west/index.html

**OHCHR.** 2025. "Impact of Disinformation on Human Rights in Ukraine." Office of the High Commissioner for Human Rights." https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/advisorycommittee/cfi-disinformation/subm-impact-disinformation-enjoyment-sta-ukraine.docx

**OSCE Delegation France.** 2024. "Joint Statement on Safety of Journalists and Freedom of the Media." https://osce.delegfrance.org/Joint-Statement-on-Safety-of-journalists-and-Freedom-of-the-Media-delivered-at

**OSCE Permanent Council.** 2023. "No. 1452 Vienna, 23 November 2023: Russian Federation's Ongoing Aggression Against Ukraine." https://www.government.is/library/09-Embassies/Vienna/1452%20PC%20Meeting%2C%2023%20November%202023%20%28e%20Russian%20Federation%E2%80%99s%20Ongoing%20Aggression%20Against%20Ukraine%29.pdf

**Pomerantsev, Peter, and Michael Weiss.** 2014. "The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money." Center for European Policy Analysis Report. https://www.ned.org/events/the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and-the-menace-of-unreality-how-the-kremlin-weaponizes-information-culture-and/

**RAND Corporation.** 2024. "Ukrainian Resistance to Russian Disinformation." RAND Research Report RRA2771-1. https://www.rand.org/pubs/research_reports/RRA2771-1.html

**Reuters.** 2022. "Kremlin Says Bucha Is 'Monstrous Forgery' Aimed at Smearing Russia." Reuters. https://www.reuters.com/world/europe/putin-ally-says-bucha-killings-are-fake-propaganda-2022-04-05/

___. 2024a. "Russia Focusing on American Social Media Stars to Covertly Influence Voters." https://www.reuters.com/world/russia-focusing-american-social-media-stars-covertly-influence-voters-2024-09-09/

___. 2024b. "US Justice Dept Says It Disrupted Russian Social Media Influence Operation." https://www.reuters.com/world/us/us-justice-dept-says-it-disrupted-russian-social-media-influence-operation-2024-07-09/

___. 2025. "Russia-linked AI Websites Aim to Dupe German Voters, Study Finds." https://www.reuters.com/world/europe/russia-linked-ai-websites-aim-dupe-german-voters-study-finds-2025-01-23/

**Surdyk, Krzysztof.** 2022. "Intelligence in hybrid warfare." Ostrowiec Świętokrzyski: Wydawnictwo WSBiP.

**US Department of State.** 2025. "Ukraine and Russia." https://2021-2025.state.gov/ukraine-and-russia/

**US Mission OSCE.** 2024. "On the Russian Federation's Malign Activities and Interference in the OSCE Region." https://osce.usmission.gov/on-the-russian-federations-malign-activities-and-interference-in-the-osce-region/

**Zanders, Jean Pascal.** 2023. "The Biological and Toxin Weapons Convention Confronting False Allegations and Disinformation." SIPRI Paper No. 85. https://www.sipri.org/publications/2023/eu-non-proliferation-and-disarmament-papers/biological-and-toxin-weapons-convention-confronting-false-allegations-and-disinformation

**Funding Information**

The author declares that no funding or financial support was received from any organization, institution, or individual for the research, design, execution, or writing of this work.

**Conflict of Interest**

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

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# "Sovereign Chișinău or Abyss with NATO" Moscow and the Moldovan EU Referendum 2024

**MA, Doctoral Researcher, Nico LAMMINPARRAS***

*University of Helsinki / Doctoral Program for Political, Societal, and Regional Change
e-mail: nico.lamminparras@gmail.com

## Abstract

The Moldovan EU referendum in October 2024 proved a page-turner; the Yes votes won by a thin margin. Russia was the first to condemn the process. In this article, I apply discourse analysis to scrutinize the language of the Russian MFA through the utterance of its spokesperson, Maria Zakharova. Intermittently, securitization schemes are employed. My aim is to divulge Moscow's standpoint on Moldova via the maneuvers that Zakharova takes advantage of in her official statements.

Zakharova's stratagems vary. She claims the referendum failed to meet the European norms, i.e., the EU alignment threatens core civil rights. Thereafter, Zakharova turns confrontational and views diplomacy as a conflict. This echoes Putin's views on a Chisinau with unbreakable ties with Russia; Moldova would no longer enjoy sovereignty in the EU. Once Zakharova poses diplomacy as a movement, she exhorts the Moldovans to counteract the true motive behind "the Western meddling". It is no more, no less, than the NATO enlargement.

**Keywords:**

Russia; Maria Zakharova; Moldova; EU; referendum; NATO; Discourse analysis; Securitization.

**Article info**

Received: 12 May 2025; Revised: 10 June 2025; Accepted: 12 June 2025; Available online: 27 June 2025

Citation: Lamminparras, N. 2025. "«Sovereign Chișinău or abyss with NATO». Moscow and the Moldovan EU referendum 2024" *Bulletin of "Carol I" National Defence University*, 14(2): 33-46. https://doi.org/10.53477/2284-9378-25-14

A mere week after the outbreak of the war in Ukraine in 2022, Moldova officially applied for EU membership. The Moldovan president, Maia Sandu, highlighted the will of the nation to "live in peace, in democracy and prosperity, as part of the free world". Accordingly, since the folks see their future in the European Union, it constitutes "a fundamental national objective" (Sandu 2022; Sandu's "consoling" discourse circa the outbreak of the war, see Lamminparras 2025, 200–201, 203–205). While the step was warmly greeted by Brussels, Moscow's stance proved ambivalent. Or in the words of President Putin, "the EU is not a military organization, a military-political block, unlike NATO. We have nothing against it [the EU]" (Putin 2022a). As late as September 2022, President Putin noted in passing "the historical proximity" between Russia and Moldova (Putin 2022b). The problem turned out to be the EU's recent evolution, as insisted on by the Russian Foreign Minister Sergey Lavrov. According to Lavrov, the discussions of an EU force, independent of the US and NATO, went on for years. However, the talks "degenerated" into cooperation with the very NATO. Now, even the non-aligned member countries are obliged to allow NATO contingents and their equipment to transit their soil (Lavrov 2022; cf. Lavrov and his deputy on Russian troops in Moldova, see Lamminparras 2024a, 166–168, 175, 178, 180–185). Conversely, the Moldovan National Security Strategy, at the time under review, not only condemns the Russian invasion into Ukraine, Moscow's meddling in the Moldovan politics and the Russian troops in Transnistria, but holds both the EU and NATO as "elementary pillars of the European security" (SNN, 2–3, 5–6, §13.3; for the envisioned Western collaboration see SNN, 17–18, 24; the Strategy was adopted in mid-December 2023). Thus, the paradox began to emerge, well before the plebiscite-to-come.

As such, the legal pattern of the referendum was flat, as the factual bid projected to modify the Constitution. The preamble was to be amended with a reconfirmation of "the European identity of the people of the Republic of Moldova" and with a declaration of "the integration into the European Union" as the country's "strategic objective". Likewise, a new Title V was to state the legal proceedings; it stipulated the "priority" of the EU obligations over the national ones, in case of "conflicting provisions" (Parlamentul Republicii Moldova 2024). Thence, the question in the plebiscite ballots crystallized in acceptance or rejection. The options were *DA*, 'yes' or *NU*, 'no', which the voter expresses by stamping *Votat* in the adjacent empty circle.

Unexpectedly, throughout the evening of October 20, 2024, the referendum turned into a thriller. Only on October 21, 2024, at 8 o'clock, the acceptance of the constitutional reform gained a majority of a few hundred ballots, and it only increased along the tabulation of diaspora votes (Lamminparras 2024b). Ultimately, of the valid ballots, 50,35 percent were cast for the constitutional amendments whilst 49,65 percent rejected the changes (CEC 2024). Substantially, this outcome reiterates the thesis of Sergeyev a decade ago: the conflict by the Dniester is not about ethnicity or nationality; rather, it is a confrontation of two larger perceptions of inheritance. While the pro-Romanian élite of Moldova stands for the Latin

roots, it simultaneously promotes the country's age-old Europeanness. Contrastively, the Russian-speakers view themselves as an inalienable part of the string of Slavic generations – or more exactly, the Russian World (Sergeyev 2015, 13).[1]

It was the Russian MFA to first issue a statement on the referendum in the evening of October 21, 2024. Markedly, zero comments were voiced by President Putin. After two days, the MFA again commented on the subject, and a week later, in anticipation of the presidential run-off on November 3, 2024, the Ministry recapped its stance. Two commentaries were published after the run-off. (Zakharova 2024a; Zakharova 2024b; Zakharova 2024c; Zakharova 2024d; Zakharova 2024e.) Of all these, the latter two primarily concern the presidential run-off. The reason is plain: on October 31, 2024, the Moldovan Constitutional Court validated the results of the plebiscite (CCM 2024). Curiously, even the Foreign Intelligence Service of the Russian Federation later published its assessment on the double polls in Moldova (SVR 2024).

Therefore, to track the Russian fresh stance on Moldova's EU-referendum and its Western integration, it proves imperative to explore the MFA's – or to be exact – Zakharova's utterance. Throughout this study, discourse analysis, as largely defined by Ricoeur and Fairclough, is applied to the public speeches and statements of Maria Zakharova. To a lesser extent, I employ securitization patterns to hint at the spokesperson's in-depth stimuli. The aim is to examine Zakharova's language and communication to unravel the strategic narratives and potential inconsistencies in Moscow's stance on Moldova. In addition to official claims of human rights violations, the discourse analysis reveals that Zakharova views diplomacy as a struggle and as a motion. Also, she takes advantage of "Russophobia". The core objective is to encumber Moldova's West-bound integration – a serious threat to Moldova's sovereignty. In order to avoid tautology and facilitate the audience's understanding of the events, the chapters are organized thematically. Thus, I hope to foster knowledge on the Russian present (geo)political reasoning on the Dniester region. Altogether, I tend to illuminate the complex questions that prospectively arise during Chisinau's European path; not least in attendance of the Moldovan parliamentary elections, to be held on September 28, 2025.

## 1. Research background

In this "technical" chapter, I first define the abbreviations and acronyms utilized in my text. Then, I briefly discuss the prior research and findings on the Russian MFA's articulation regarding today's Moldova. Notably, this

[1] The conflict in Southern Moldova – known as the Gagauzian conflict – evolved within a similar framework (Bejan 2022, 224–225, 229–238). However, the Gagauz stance on the EU-referendum of 2024 merits its own study.

article focuses on Moscow's *current political* utterance, and not on that historical one. A separate manus on Russia's views – i.e., time and again Zakharova's interpretations – on the Moldovan past is under review elsewhere. It is also worth mentioning that I observed and commented on the referendum and the elections live and proactively during the entire period from October 20 to November 4, 2024. Since the electoral processes themselves do not constitute the topic of this article, I exclude my first-hand analyses (destined for the native audience); nevertheless, some features of those may manifest here. Equally, as the primary material is presented above, I here limit myself to disclosing the method.

### *1.1. Abbreviations*

| | | |
|---|---|---|
| CCM | Curtea Constiţutională | Constitutional Court (MD) |
| CEC | Comisia Electorală Centrală | Central Election Commission (MD) |
| MFA | | Ministry of Foreign Affairs (RU) |
| Parlamentul | Parlamentul Republicii Moldova | Parliament (MD) |
| SVR | Sluzhba vneyshney razvedki | Foreign Intelligence Service (RU) |

### *1.2. Prior research*

Noteworthily, it was the spokesperson of the MFA, Maria Zakharova, to address the Moldovan topics, not President Putin, nor the Kremlin. Overall, during the years 2022–2024, Putin less than twenty times tackled or mentioned Moldova (for Putin's Moldova-argumentation see Lamminparras 2024c). Within the MFA, it is intriguing that the very Minister of Foreign Affairs, Sergey Lavrov, remains tacit on these topics. Despite her both nationally and internationally visible position, it is somewhat strange that most of the Zakharova inquiries are produced in Russia. As most of them date to the years before the war in Ukraine, this article to a minor extent refers to updates and widens our topical knowledge, in Russia and abroad.

In the mid- and late 2010s, Gorbacheva and Zaynullina explored Zakharova's career and manners, lexicon included. Gorbacheva and Zaynullina highlight that the spokesperson has served in her office since August 2015 and is the first woman to preside over the Department of Information and Press of the Russian MFA. In addition to the traditional channels, Zakharova is renowned for her communication in TV talk shows and on social media (Gorbacheva 2016, 7; Zaynullina 2018, 166). Martynenko and Mel'nikova rather focus on Zakharova's appearance. These two juxtapose Zakharova and her Western counterpart, Jennifer Psaki (Martynenko and Mel'nikova 2016).

Zakharova's (use of) language became a topic of discussion circa 2020. Sandler differentiates the various techniques that Zakharova applies, such as graduation and reiteration. Besides that, Sandler illuminates the discursive stratagems the spokesperson utilizes, such as diplomacy as conflict or an explanatory unfolding (Sandler 2022). After the outbreak of the war in Ukraine, Belova-Dalton has investigated Zakharova's communication on the Crimean as well as the Donbas

conundrums (Belova-Dalton 2023). In late 2024, I explored Putin's understanding of the Russians by the Danube from the sixth to the late eighteenth century. As I analyze the Russian president's views on Chisinau's present politics, the article provides for comparison (Lamminparras 2024c). Kireyeva and Pikuleva determine that due to her vivid tongue, Zakharova has become one of the most quoted Russian diplomats. Or better said, "the main media face" of the MFA (Kireyeva and Pikuleva 2019, 21).

***1.3. Discourse analysis***

As for the methodology – discourse analysis –, I widely allude to Norman Fairclough's theorization on the (use of) language in a complete nexus with its social frames. Fairclough divides his idea into three levels. On the textual one, the attention is paid to solitary words and phrases. Secondly, the so-called production level includes the process of any given presentation and the resources behind it. Thirdly, on the sociocultural level, the researcher is interested in the presentation's links with the past and present. Simultaneously, the presentation further builds its social environment. (Fairclough 1992, 1, 38, 62–63.) Eskola and Ricoeur explain this interdependence in a more usual fashion. Firstly, the essence of simple words emerges from the context in which they manifest (Eskola 1996, 65, 127). Ricoeur concludes that a full maxim then refers "beyond itself", to the (linguistic) environment in question (Ricoeur 1976, 6–7, 20, 88).

Since we speak of one of the key Russian ministries, resources are readily available. Hence, I concentrate on the textual and the sociocultural levels throughout the investigation on Zakharova's referendum-related discourse. To summarize the context, as Eskola puts it, it is essential to differentiate the idioms, allusions, and omissions that Zakharova pronounces. The auxiliary questions are as follows:

- How does the spokesperson describe the Moldovan referendum?
- What kind of implications does Zakharova's voice convey?
- How does the sociopolitical environment affect her utterance?

To ensure the informativeness and the authenticity of the linguistic framework, I employ Zakharova's live discourses, held in Russian. Once set in standard Word parameters, they number a dozen pages, or 3,887 words. As discourse analytical principles prefer ample and thorough corpuses, the choice provides for an appropriate source material. The author retains solid copyrights for the translations from Russian, Romanian/Moldovan, and other tongues. To precisely trace the course of the events and to trace the point of reference of Zakharova's implications, I include data from the electoral and other local authorities.

Now, there lies a profound link to securitization schemes. By and large, Balzacq suggests that global politics is extensively conducted via language (Balzacq 2011, xiv; for the securitization schools and their disputes, see Langenohl 2019). According to Stritzel, security is often perceived as a political reading within a deliberate framework (Stritzel 2014, 16). To simplify, a so-called 'securitizing actor' summons

imagery, policy tools, and symbols to stimulate his/her 'audience' to foster concerns about a 'referent object' under threat [say the native soil or civil rights]. The securitizing actor delivers the menace – 'referent subject' – in such maneuvers that a given policy is required to impede its existence (Balzacq 2011, 3). Here, we reach 360 degrees. As the discourse analysis reveals, every text echoes its links with the past; in tandem, it generates the present. In this study, Zakharova is the obvious actor while the audience consists of journalists who attended/read each of her comments; of course, they personalize the Russian and Moldovan societies (perhaps, the Globe too). Thence, whilst I explore Zakharova's appearances, we may partially track the impetuses of her securitizing manners. Unfortunately, a distinct examination of Zakharova's securitization acts, whether in these texts or in general, is rescinded due to the limited space. Hence, I only indicate such sections that may serve as a starting point for later inquiries. Entirely, this joint approach results in an assembly of speeches, narratives, and inferences voiced by Zakharova, diligently probed, set in their adequate ties, and positioned in a thorough account.

## 2. "Non-European circumstances"

It is of primary interest that Moscow challenges the entire legitimacy of the referendum. First, the electoral campaign was far from democratic, and the fundamental human rights (referent object) were violated. Here, Zakharova sharply depicts the unilateral actions taken by Chisinau's pro-European government (referent subject). One might differentiate an echo from Putin's notion of an equally one-sided campaign. According to the Russian president, the Moldovan leadership rejects its Moldovan inheritance and instead, perceives itself as Romanian. Overtly, Putin calls this "a complete forfeiture of the country's identity" (Lamminparras 2024c, 106). Just as the president's words, so does Zakharova's idiom exhibit a high-style lexicon, e.g., the jurisprudence (Gorbacheva 2016, 9).

> By the Moldovan authorities, the electoral campaign was conducted through anti-democratic, totalitarian methods. -- The Moldovan leadership -- carried out repressions against opposition politicians and independent media (Zakharova 2024a).
>
> Despite the massive repressions of the opposition and the independent media, undertaken by the authorities in Chisinau… (Zakharova 2024b).
>
> The current electoral campaign in this country is characterized by unparalleled repression. -- of political actors, independent media, opposition, social activists, and people who tend to defend the truth (Zakharova 2024c).

According to Sandler (2022, 116), Zakharova often utilizes such discursive techniques that reinforce each other, such as repetition and graduation. Seemingly, she here commences with a rather high-level allusion to the authoritarian élite of Moldova, but then three times reiterates the term 'repression'.

It is likely that after the initial reaction, which may have proved too general, Zakharova tends to further underscore the breach of basic civil rights in Moldova. Not least, because the number of strata, allegedly subjected to the oppressive measures, increases. Likewise, after the presidential run-off on November 3, 2024, Zakharova pronounced a qualitative graduation. She noted that the suppressed media was "mostly Russophone" (Zakharova 2024d). In other words, Zakharova postures the menace to have turned into an essential one. Now, it is the possibility to transmit and receive information in Russian – implying the entire Russian-speaking community in Moldova – that is at stake (the ultimate referent object?). Yet, those "defending the truth" remained opaque – they stand for the veracity of…? Generally, Zakharova portrays Moldova as a state with scarce rule of law and with restricted freedom of the media and speech. As these values are so cherished in Europe, she covertly claims the country fails to fulfil the EU membership criteria.

Amid these, the violation of fundamental rights was not limited to Moldova alone. The Moldovans residing in Russia were virtually deprived of the right to go to the polls. "The culmination of Chisinau's anti-Russian campaign"

> -- was the decision, taken under a contrived pretext, to open in Russia, where 300 to 500 thousand Moldovans live, merely two polling stations (Zakharova 2024a).
>
> A particular cynicism is involved in the fact that those Moldovans who decided to travel to Moldova to vote were deprived of this possibility. Already by the Russian-Latvian boundary, they were pushed back under the pretext of «EU security threat» (Zakharova 2024e).

Intriguingly, here we observe Zakharova's manner to pose diplomacy as "an artistic representation". It is the voice 'culmination' that stems from this context (Kireyeva and Pikuleva 2019, 24–25). To underline the inequality, Zakharova compares the procedure with those around the Globe.

> The discrimination of the Moldovan voters living in Russia, by the official Chisinau, merits particular attention. -- For comparison: in Western Europe and Northern America, where likewise some 500 thousand Moldovans live, more than 200 stations were set up, while in several countries it was permitted for the Moldovan citizens to vote by mail (Zakharova 2024d).

Per se, the numbers are correct. In total, 234 polling stations operated abroad. Of these, only two stations were in Russia, both in Moscow, in the premises of the Moldovan consular service (CEC 2024). Repeatedly, with her constant reminders of this visible incongruity, Zakharova implies Moldova's ambiguous commitment to European standards and factually hampers Chisinau's EU path. One might, with good grounds, wonder whether a couple of polling stations, say in Saint-Petersburg, would not better have met the international norms. Had the outcome turned out the opposite or not is not relevant in this interpretation. Not even for Zakharova: in

any case, it is the core civil rights – referent object – that were severely breached, in Moldova and elsewhere.

## 3. Western interference

At the same time, by juxtaposing the number of polling stations back home and overseas, the spokesperson initiates a confrontation. This falls in stark contrast with Sandler's thesis of Zakharova's diverse communicative resources under the circumstances of a fierce military-political and cultural-ideological contest between the Russian World and the collective West (Sandler 2022, 116). In other words, Zakharova firmly neglects her capabilities of building balance or settling. Instead, she opts for the metaphorical model of diplomacy as a struggle, if not an outright war. It is mainly the allusion to "the anti-Russian campaign" that points to this (Kireyeva and Pikuleva 2019, 22–24). Not only is the voice "campaign" associated with warfare, but the implication is that there exists a united movement with a common will (second referent subject) to combat Russia and Russianness (second referent object).

According to Robinson, before the year 2012, the Russian MFA seldom utilized the concept of "Russophobia" as an argument. Such discourse drastically augmented after 2012, that is, side by side with the conflicts in Crimea and in Donbas (Robinson 2019, 61, 64, 73; Zakharova on Crimea and Donbas see e.g. Belova-Dalton 2023, 69, 77, 80). Analogically, since the outburst of the full-fledged war in Ukraine and the subsequent isolation of Russia, one might expect this pretension to increase. However, in the case of Moldova, this kind of utterance appears minuscule; Zakharova enhances the international competition with milder locutions. For example, to the surprise of many, Zakharova thrice admits that there was a substantial interference in the Moldovan elections and the plebiscite. Though she leaves no doubt of the guilty one:

> All this occurred amidst an unconcealed meddling of the West in the electoral process in Moldova (Zakharova 2024a).
> -- The only thing they are right – an unprecedented meddling, truly, took place. Though, from the USA and the EU's side (Zakharova 2024b).
> All this occurs along the massive meddling of the «collective West» in the internal affairs of the republic (Zakharova 2024c).

Since the verbs are in the past form, apart from the latest commentary, these lines appear to feature an explanatory nature, as described by Gorbacheva. Also, the descriptive and narrative markers – e.g., 'amidst', 'truly', and 'Though' – assist in underscoring the message. (Gorbacheva 2016, 10.) Somewhat paradoxically, the expressions still turn as acid as vivid and rather resemble accusations. Paraphrasing Sandler (2022, 116), this impression is further hardened by repetition. Moreover, the Western interference took visible forms. According to Zakharova, during their many

visits to Chisinau, the leaders of the EU-member states conducted "open agitation for Moldova's current headship" (Zakharova 2024a), and the "emissaries" of the US and the EU brought in money (Zakharova 2024b). The spokesperson implies that the pro-Sandu and the pro-European rallies were welcomed, if not encouraged. I.e., she covertly recaps the arguments on Moldova's one-eyed rule (referent subject again) and its failure to observe fundamental rights (referent object again). At the same time, Zakharova raises the question of where to draw the line between legitimate financing from abroad and that disguised as such. Most likely, this clandestine reference was aimed at alleviating the Moldovan President Sandu's allegations of criminal and foreign meddling in the plebiscite (Privesc 2024a; cf. Zakharova 2024b).[2]

The climax of Zakharova's quarrelsome discourse is her account of the referendum's tabulation. Initially, she points out "the dynamics of the voting":

> With 71,25% of the ballots processed, the gap persisted: «for» – 44,68%, «against» – 55,32%. Then, it swiftly – and inexplicably to many in Moldova – started to shrink, and after the processing of 99% of the protocols, the outcome turned «for» – 50,3%, «against» – 49,7% (Zakharova 2024a).

Judging by the plain numbers, the referendum resulted in indecision. Of the valid votes, 50,35 percent were cast in favor of the constitutional changes, and 49,65 percent were against. The gap is less than eleven thousand ballots (CEC 2024). Without overtly stating it, Zakharova likens "the favorable outcome" to a conspiracy since it was "obtained by the authorities with a gap less than 1%, through a dire mobilization of votes in the overseas diaspora" (Zakharova 2024e; see also Zakharova 2024c). Again, it is the Moldovan pro-EU leaders to suppress the will of the citizens.

Whilst we need to figure out the plotters from the astute implication, Zakharova leaves no uncertainty over the real name of this phenomenon. Following her deduction, it constituted a premeditated "falsification" (Zakharova 2024a, 2024b). To enforce the claim, Zakharova now transitions to describe diplomacy as "propulsion" or "route" (see Kireyeva and Pikuleva 2019, 22–23). The likely aims of this choice are to warn the Moldovans and to exhort them to counteract the country's current course. Again, the similarity with Putin's assessments on Moldova's political life is eye-catching. A mere year afore, Putin three times encouraged the Moldovans to impede the country's EU alignment. Rigorously, Putin advised not to vote for "those who aspire to relinquish a significant portion of their sovereignty to other countries"; it shall end in the loss of self-determination (Lamminparras 2024c, 107–108, 111–112). Whether

[2] It is of a major interest that Sandu's main opponent, the pro-Eastern ex-state attorney Alexandr Stoianoglo, immediately emulated the allegations. Also, he was the first to blame Sandu's government for the repressive measures. (Privesc 2024b.) I warmly encourage my fellow academicians to delve into Stoianoglo's political views and discourse during 2024, to speak nothing about his career as State Attorney.

this is yet realized or not represents a question itself. In contrast to the president, Zakharova explicitly stated the final objective of the rigged referendum. That is, to turn Moldova into "a Russophobic NATO appendage", without sovereignty (Zakharova 2024a).

## Conclusions

There's no suspicion over Moscow's expertise in the field of public communication, as embodied in Maria Zakharova. Her position as the prime commentator of the Russian Ministry of Foreign Affairs is founded on her capability to perform in multiple channels, TV shows, and social media. Her idiom flexibly varies from one register to another, and from a daily to a specific lexicon. In addition, the discourse on the Moldovan EU referendum demonstrated she is able to navigate between a readily confirmatory strategy and a confrontational one. Eruditely, she inserts securitization schemes within these stratagems.

Zakharova, in her guise, Russia, condemns the referendum as profoundly illegitimate. The basic civil rights (referent object) were violated, both in Moldova and overseas. The spokesperson underscores the repression of the opposition, unnamed dissenting individuals, the independent media, etc. There is no doubt over who undertakes these oppressive measures – the Moldovan pro-Western élite (referent subject). I.e., the very same circles that, with an equally unilateral push, promote a Romanian–not–Moldovan identity, as Putin in 2023 blamed. By this time, Moscow had become increasingly aware of the EU's alleged evolution toward an instrument to advance NATO's foothold. Later, Zakharova mentions that the repressed news agencies predominantly consisted of Russian-language media. Thus, what is in danger is a whole Russian-speaking community (the true referent object?). Logically, Moldova's decision to open a mere two polling stations in Russia, where 300 to 500 thousand kinsmen have their residence, constituted the "culmination of Chisinau's anti-Russian campaign". With these claims, Moscow seeks to hinder Chisinau's EU integration. As Moldova purposefully breaches fundamental freedoms, it does not comply with European standards.

Here, Zakharova applies two distinct yet concomitant strategies. The voice 'culmination' emerges from her view on diplomacy as an artistic performance, whereas the term 'campaign' indicates diplomacy as a conflict, if not sheer warfare. Through these choices, Zakharova proceeds to the confrontational approach. It is the alleged "Russophobia" that implies a larger entity (the genuine referent subject?) to combat Russia and its core beliefs, with Moldova as one of its tools. For example, the slightly bitter judgment of the polling stations opened in the Americas and Europe mainly confirms the rift. For a comparable number of Moldovan expatriates, there were more than 200 stations. Nonetheless, as it was precisely these diaspora votes that finally turned decisive, with a margin of less than 0,4 percent, Zakharova

insinuates an orchestrated voting in the West. Moreover, the representatives of the US and the EU publicly advocated the cause of the incumbent President Maia Sandu and her government, to speak nothing about the Western financing. Besides its concrete reference, the latter argument serves as a reply to Maia Sandu's allegations of foreign and hostile interference.

To summarize, Zakharova passes to perceive diplomacy as a yet ongoing move or path. Unlike in the case of Crimea and Eastern Ukraine since 2014, she utilizes milder accusations. In this respect, it seems that the spokesperson, – or accurately, Moscow – benignly relates to the Moldovan ordinary people. Just as Putin exhorts these to hamper the country's EU path, Zakharova infers that the Moldovans, especially those residing within the republic, are victims of a deception. To deepen these preliminary findings, I propose a separate investigation and/or comparison, both in the case of this topic and of Zakharova's (further) securitization maneuvers. Not least because by associating the true scope of the "Western meddling" with Chisinau's Euro-Atlantic aspirations, Zakharova in fact urges the local people to cherish a sovereign Moldova – or to perish with NATO.

## References

**Balzacq, Th.** 2011. *Securitisation Theory: How Security Problems Emerge and Disappear.* London and New York: Routledge.

**Bejan, Şt.** 2022. *Găgăuzii: origini, evoluţie şi aşezarea în Sudul Basarabiei* [The Gagauz: origins, evolution, and settlement in Southern Bessarabia]. Chişinău: Editura Arc.

**Belova-Dalton, O.** 2023. "Putin's extremist regime and its securitisation of the invasion of Ukraine through the label of terrorism." *Security Spectrum*, 22: 53-98. Tallinn: Sisekaitseakadeemia.

**Borţun, D., and Săvulescu, S.** 2009. *Analiza discursului public* [Analysis of public discourse]. Bucureşti: Școala Naţională de Studii Politice şi Administrative.

**CCM.** 2024. *Examinarea sesizării privind confirmarea rezultatului referendumului republican* [Examination of the confirmation of the result of the nationwide referendum] | *212d/2024.* Chişinău.

**CEC.** 2024. "Rezultatele referendumului republican constitutional [The results of the nationwide constitutional referendum]." Chişinău.

**Eskola, T.** 1996. *Uuden Testamentin hermeneutiikka. Tulkintateorian perusteita* [The hermeneutics of the New Testament. Fundaments of the interpretation theory]. Helsinki: Yliopistopaino.

**Fairclough, N.** 1992. *Discourse and Social Change.* Cambridge: Polity Press.

**Gorbacheva, Y.** 2016. "Rechevoy zhanr «Diplomaticheskiy kommentariy» s pozitsii diskursivnoy performativnosti" [Discursive genre «Diplomatic commentary» from the perspective of discursive performativity]." *Kommunikativnyje issledovanija* [Communications studies], 2:7-16. Omsk: Omskiy gosudarstvennyj universitet im. F. M. Dostoyevskogo.

**Kireyeva, A., and Ju. Pikuleva.** 2019. "Diplomaticheskie otnoshenija v metaforicheskom opisanii (na materiale vyskazyvaniy Marii Zakharovoy)" [Diplomatic relations as metaphorical depiction (in the public speeches of Maria Zakharova)]. *Molodye golosa* [Young voices], 8:21-25. Yekaterinburg: OOO Izdatelskiy Dom «Azhur».

**Lamminparras, N.** 2025. Blodig flyter Dnjestr. Kriget 1992 i Moldaviens & Transnistriens diskurser 30 år efteråt [And bloodstained flows the Dniester. War 1992 in Moldova and Transnistria's discourse 30 years after]. *Tiede ja ase* [Science and arms]. Vol 2024, no 82: 192–222. Helsinki: Finnish Society of Military Sciences. https://journal.fi/ta/issue/view/12282/2824.

___. 2024a. Dnestrin epätoivotut vartijat. Moldovan & Transnistrian presidentin diskurssi Venäjän sotilaista Moldovassa 2021 [Dniester's unsolicited sentinels. The discourses of the presidents of Moldova and Transnistria on the Russian military in Moldova in 2021]. *Tiede ja ase* [Science and arms], Vol 2023, No 81: 155–190. Helsinki: Finnish Society of Military Sciences. https://journal.fi/ta/issue/view/10976/2313.

___**.** 2024b. Vilppi ei peitä Moldovan EU-etoa [Fraud doesn't cover Moldova's EU-indifference]. *Uusi Suomi*. Juuka. https://puheenvuoro.uusisuomi.fi/nico-lamminparras/vilppi-ei-peita-moldovan-eu-etoa/.

___**.** 2024c. Putin's Implicit War History of the Russians by the Danube in 500-1792. *Revista de Istorie Militară,* 3-4: 105-114. București: ISPAIM.

**Langenohl, A.** 2019. "Dynamics of Power in Securitisation: Towards a Relational Understanding." In *Conceptualizing Power in Dynamics of Securitisation*, by A. Langenohl and R. Kreide, 25–37. Baden-Baden: Nomos.

**Lavrov, S.V.** 2022. Intervju Ministra Inostrannykh del Rossii S. V. Lavrova telekanalu NTV, Sankt-Peterburg, 16 ijunja 2022 goda. St. Petersburg. https://mid.ru/ru/foreign_policy/news/1818292/.

**Martynenko, Y., and A. Mel'nikova.** 2016. "Medinye litsa vneshney politiki SSHA i Rossii: Dzh. Psaki vs M. Zakharova [Media faces of the foreign policies of the US and of Russia: J. Psak vs. M. Zakharova]." *Obshtshestvo: politika, ekonomika, pravo* [Society: politics, economy, law], 10: 16-19. Krasnodar: Izdatelskiy dom «HORS».

**Parlamentul Republicii Moldova.** 2024. "LEGE pentru modificarea Constituției Republicii Moldova [LAW on the modification of the Constitution of the Republic of Moldova]." Chisinau.

**Privesc.** 2024a. Briefing de presă susținut de candidata la funcția de președinte al Republicii Moldova, Maia Sandu, după închiderea secțiilor de votare. Chisinau. https://youtu.be/2GSm0JUgIMA.

___. 2024b. Briefing de presă susținut de candidatul la funcția de președinte al Republicii Moldova, Alexandr Stoianoglo, după închiderea secțiilor de votare. Chisinau. https://youtu.be/b6b_HsiC4vw.

**Putin (Prezident Rossii).** 2022a. Plenarnoye zasedaniye Petersburskogo mezhdunarodnogo ekonomicheskogo foruma [Plenary session of the St. Petersburg international economic forum]. St. Petersburg. http://www.kremlin.ru/events/president/news/68669.

___**.** 2022b. Tseremoniya vrucheniya veritel'nikh gramot [Conferral ceremony of the credentials]. Moskva. http://kremlin.ru/events/president/news/69379.

**Ricoeur, P.** 1976. *Interpretation Theory and the Surplus of Meaning.* Fort Worth: The Texas Christian University Press.

**Robinson, N.** 2019. "Russophobia" in Official Russian Political Discourse." *De Europa*, 2: 61-77. Torino: Università di Torino.

**Sandler, L.** 2022. "Strategija konfrontatsii v informatsionnoy voyne (na primere vystupleniy Marii Zakharovoy) [Confrontation strategy amid information warfare (with Maria Zakharova's appearances as example)]." *Kommunikatsija v sovremennom mire* [Communication in contemporary world], 20: 115-117. Voronezh: Voronezhkiy gosudarstvenniy universitet.

**Sandu (Președinția Republicii Moldova).** 2022. "Declarația Președintei Maia Sandu cu ocazia semnării cererii de aderare a Republicii Moldova la Uniunea Europeană." Chișinău. https://presedinte.md/rom/discursuri/declaratia-presedintei-maia-sandu-cu-ocazia-semnarii-cererii-de-aderarea-a-republicii-moldova-la-uniunea-europeana.

**Sergeyev, A.** 2015. *Pridnestrov'ye segodnya: problemy i perspektivy zhiznedejatel'nosti* [Pridnestrovie today: problems and perspectives of viability]. Moskva: RISI.

**Stritzel, H.** 2014. *Security in Translation: Securitisation Theory and the Localisation of Threat.* St. Andrews (UK): University of St. Andrews.

**SVR.** 2024. "OBSE pokryvayet mashtabnye narusheniya na vyborah v Moldavii" [OSCE veils massive irregularities in the elections in Moldova]. Moscow. http://svr.gov.ru/smi/2024/10/obse-pokryvaet-masshtabnye-narusheniya-na-vyborakh-v-moldavii.htm.

**Zakharova.** 2024a. "Kommentariy ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy po itogam pervogo tura prezidentskikh vyborov i konstitutsionnogo referenduma v Moldavii". Moscow. https://mid.ru/ru/foreign_policy/news/1976983/.

___. 2024b. "Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy." Moskva, 23 oktyabrya 2024 goda. Moscow. https://mid.ru/ru/foreign_policy/news/1977268.

___. 2024c. "Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy." Moskva, 30 oktyabrya 2024 goda. Moscow. https://mid.ru/ru/foreign_policy/news/1978331/.

___. 2024d. "Kommentariy ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy o vtorom ture prezidentskikh vyborov v Moldavii." Moscow. https://mid.ru/ru/foreign_policy/news/1979108/.

___. 2024e. "Otvet ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy na voproz CMI o stituatsii v Moldavii." Moscow. https://mid.ru/ru/foreign_policy/news/1979818/.

**Zaynullina, A.** 2018. "Mediaobraz Marii Zakharovoy kak instrument informatsionno-kommunikatsionnoy politiki MID RF [Media image of Maria Zakharova as an instrument of information and communication policy of the MFA of the Russian Federation]." *Redaktsionnaya kollegiya* [Editorial collegium]. 165-168. Sankt-Petersburg: Sankt-Petersburgskiy gosudarstvenniy ekonomitsheskiy universitet.

**ACKNOWLEDGEMENTS**
I express my gratitude to Professor Emeritus Timo Vihavainen for methodological guidance.

**FUNDING INFORMATION**
N/A

**CONFLICT OF INTEREST STATEMENT**
The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**DATA AVAILABILITY STATEMENT**
The data that support the findings of this study are openly available in the internet.

**DECLARATION on AI use (if applicable)**
N/A

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Towards a Taxonomy of Hybrid Warfare: Lessons from Crimea and the Donbas

**Lecturer Tarık SOLMAZ, PhD***

*Turkish Military Academy, Ankara, Türkiye
e-mail: tarik.solmaz@msu.edu.tr

## Abstract

While "hybrid warfare" has attracted considerable interest among defense intellectuals for more than a decade, it still appears conceptually flawed. The main reason for this is that hybrid warfare remains a catch-all concept encompassing various types of actions. As such, the notion of hybrid warfare seems overly broad for academic analysis and national security planning. A classification of hybrid warfare is essential to distinguish its principal types. The research question for this article is, therefore: How can hybrid warfare be classified based on its modus operandi? In addressing this question, the article proposes a taxonomy based on David Kilcullen's ideal types of counterinsurgency, namely, population-centric and enemy-centric models, given that hybrid warfare can manifest in two main forms, either as a direct challenge to military forces or as a malign influence on civilian populations and decision-makers. To illustrate this distinction, it examines two classic cases of the hybrid mode of warfare: Russia's annexation of Crimea and covert occupation of the Donbas region. The findings suggest that Russia's annexation of Crimea reflects a population-centric hybrid warfare approach, because it was essentially based mostly on non-violent actions rather than violent conflict. On the contrary, Russia's covert occupation of the Donbas region indicates a more violent, enemy-centric model as it prioritizes military dominance.

**Keywords:**
hybrid warfare; David Kilcullen; population-centric; enemy-centric; Crimea; Donbas.

**Article info**
Received: 15 May 2025; Revised: 5 June 2025; Accepted: 10 June 2025; Available online: 27 June 2025

Citation: Solmaz, T. 2025. "Towards a Taxonomy of Hybrid Warfare: Lessons from Crimea and the Donbasw" *Bulletin of "Carol I" National Defence University*, 14(2): 47-61. https://doi.org/10.53477/2284-9378-25-15

Since Russia's arm's-length operations in Crimea and Donbas in 2014, the term "hybrid warfare" has attracted significant attention in Western strategic circles. Yet, although its usage has become increasingly widespread, the idea of hybrid warfare continues to present analytical challenges. The prevailing definition of hybrid warfare is so broad that it undermines its usefulness in both academic analysis and policymaking (Wither 2016, 74). Today, the hybrid model of warfare is generally portrayed as a method of achieving political objectives by employing a blend of military and non-military means while remaining below the threshold of large-scale, force-on-force military operations (Popescu 2015, 1; European Commission 2016, 2; NATO 2024). Based on this perspective, hybrid warfare may take different forms and be implemented in diverse settings. For this reason, the case studies commonly cited as examples of hybrid warfare are often markedly different from one another, and – aside from their classification under the hybrid label – have little in common.

This article seeks to contribute to the conceptual development of hybrid warfare by proposing a new taxonomy that clarifies the differences between different types of hybrid warfare. To achieve this, it applies David Kilcullen's renowned taxonomy, initially used in counterinsurgency, to distinguish between population-centric and enemy-centric models within the context of hybrid warfare. He delineates the population-centric approach, viewing counterinsurgency as "fundamentally a control problem, or even an armed variant of government administration" (Kilcullen 2007). The core objective is to secure control over both the population and the surrounding environment. While the methods employed within this model can range from more forceful to more conciliatory ones, the core principle is that achieving control over the population is crucial, with other goals following as secondary.

In contrast, Kilcullen (2007) views the enemy-centric approach as a form of conventional warfare, with the main objective of defeating the enemy. That being said, the enemy-centric approach to counterinsurgency also includes efforts to gain control over the population and its surrounding environment. Yet, while it overlaps with the population-centric model in particular aspects, its central emphasis lies on ensuring the enemy's military defeat takes precedence over all other goals.

Drawing on Kilcullen's conceptual model, this article proposes a new taxonomy of hybrid warfare by categorizing it into two subtypes according to the nature of actions (disruptive vs. destructive) and their principal targets: *population-centric hybrid warfare* and *enemy-centric hybrid warfare*. This classification offers a more precise and nuanced conceptual lens through which to interpret the diverse manifestations of hybrid warfare.

The remainder of this article is structured as follows: the next section reviews the literature on the definition and characteristics of hybrid warfare. This is followed by a discussion of the article's methodological framework. The subsequent section

examines two defining case studies of hybrid warfare: Russia's annexation of Crimea and covert occupation of the Donbas region. Each of the case studies illustrates a different variant of hybrid warfare. Afterwards, the findings relating to the case studies examined will be presented. The article concludes with a brief overview that summarizes the key arguments and discusses their implications for future research.

## 1. Literature Review

Hybrid warfare has become a buzzword in the Western political and academic circles since Russia's "deniable" intervention in Ukraine in 2014. However, in truth, hybrid warfare has not been the sole concept used to describe and to refer to Russia's hostile measures in Ukraine. On the contrary, there has been a broad array of concepts used for this purpose. Radin and others (2020, 2) stated that the term "subversion" provides an appropriate and helpful way to apprehend Russia's destabilizing activities in Crimea and the Donbas region. Galeotti (2019a) used George F. Kennan's construct of "political warfare" to explain the same phenomenon. Friedman (2014) referred to it as "limited war". Mazarr (2015) used the concept of "grey-zone warfare", while Connell and Evans (2015) preferred the term "ambiguous warfare." Bērziņš (2015, 157-158) pointed out that the term "new generation warfare", which is the product of Russian military thinking, captures Russian way of warfare employed in Ukraine better than any other Western-oriented concepts since "it is a methodological mistake to try to frame a theory developed independently by the Russian military as a theory developed in another country."

Nonetheless, NATO (2014) preferred the term hybrid warfare to describe Russia's destabilizing activities in Crimea and Donbas. With NATO's choice, as Libiseller (2023) has said, "hybrid warfare" became an academic fashion in Western scholarly and military-practitioner circles. In fact, the term itself had already entered the Western strategic lexicon before Russia's 2014 operations in Ukraine. It dates back to the early 1990s (Mockaitis 1990) and was popularized by Hoffman (2007) in the second half of the 2000s. In his seminal work, entitled *Conflict in the 21st Century: The Rise of Hybrid Wars*, Hoffman (2007, 14) defines hybrid warfare as a form of conflict incorporating "a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."

According to Hoffman (2007, 36), Hezbollah's mode of warfare against Israel during the 2006 Lebanon War represents a clear-cut example of hybrid warfare. He says that "Hezbollah's use of C802 anti-ship cruise missiles and volley of rockets represents a sample of what 'Hybrid Warfare' might look like (Hoffman 2007, 37). Hoffman's conceptualization of hybrid warfare primarily aimed to explain how and why a relatively weak actor had become successful against a superior conventional military force.

Hoffman's battlefield-centric understanding of hybrid warfare mainly dominated the literature until Russia's 2014 operations in Crimea and the Donbas region. However, since Russia's activities in Ukraine exhibited different characteristics from Hoffman's definition of hybrid warfare, the North Atlantic Treaty Organization (NATO) reformulated the concept to highlight the role of non-military means. During a speech in June 2014, the then Secretary General of NATO, Anders F. Rasmussen, described hybrid warfare as "a combination of covert military operations combined with sophisticated information and disinformation operations" (Rasmussen 2014). In the 2014 NATO Wales Summit Declaration, the Alliance defined hybrid warfare as "a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design" (NATO 2014).

Over time, NATO's understanding of hybrid warfare has evolved to include "strategic ambiguity" and "plausible deniability" recognizing that Russia's operations in Crimea and Donbas can be best characterized by remaining below the threshold of an outright act of war, rather than merely conceiving such warfare as a mixture of various kinetic and non-kinetic instruments. Over the past few years, NATO (2024) has characterized hybrid warfare as follows:

> Hybrid threats combine military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups, and use of regular forces. Hybrid methods are used to blur the lines between war and peace and attempt to sow doubt in the minds of target populations. They aim to destabilize and undermine societies.

Reflecting NATO's approach, hybrid warfare has commonly been understood as a method of realizing geostrategic objectives by using any combination of kinetic and non-kinetic instruments while remaining below the threshold of a large-scale conventional war. For example, the EU's Joint Framework on countering hybrid threats states:

> The concept of hybrid threats aims to capture the mixture of conventional and unconventional, military and non-military, overt and covert actions that can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare (European Commission 2016).

The majority of academic definitions of hybrid warfare also reflect the same understanding of hybrid warfare. Thus, they emphasize the concurrent and synergistic use of military and non-military instruments, while regarding remaining below the threshold of direct force-on-force confrontations as one of the defining characteristics of the hybrid mode of warfare (Popescu 2015, 1; Mumford and Carlucci 2023, 194-195). Such a conceptualization of hybrid warfare is not that different from Kilcullen's theory of liminal maneuver. For Kilcullen, liminal warfare centers on manipulating thresholds. Revisionist powers like

Russia and China seek to pursue their geostrategic objectives without crossing the threshold into war. To that end, they conduct covert and indirect operations through economic, military, cyber, and informational tools. These operations may be detected, but their agency or sponsorship mostly remains ambiguous, and therefore, unproven (Kilcullen 2020, 115-120).

With this understanding, hybrid warfare may take a broad range of shapes and be practiced in different ways. Today, the single term "hybrid warfare" has been used to describe a diverse range of strategies and tactics employed by actors with qualitatively and quantitatively different characteristics. The examples/case studies labelled as hybrid warfare span from Russia's operations in Crimea and Donbas (Fox 2017), to China's bullying activities in the South China Sea (Miracola 2018), to North Korea's aggressive behaviors towards South Korea (Kang 2020), to Iran's pursuit of regional hegemony in the Middle East (Dalton 2017). Obviously, the examples of case studies lack a clear conceptual link between them, even though they all fall under the umbrella of hybrid warfare. Given the wide scope of activities the term encompasses, developing a taxonomy would facilitate a more nuanced understanding of its diverse manifestations.

## 2. Methodology

This article seeks to advance the conceptual clarity of hybrid warfare by suggesting a new taxonomy that clarifies the differences between its various forms. To this end, it seeks to answer the following research question: *How can hybrid warfare be classified based on its modus operandi?* The article employs a qualitative research design based on a comparative case study approach. The case studies selected, namely, Russia's annexation of Crimea and its covert occupation of the Donbas region, are chosen because they represent two archetypal examples of hybrid warfare and thus offer an ideal basis for illustrating the proposed taxonomy.

In categorizing the hybrid mode of warfare, the article applies David Kilcullen's population-centric and enemy-centric models, initially developed in the context of counterinsurgency, to the field of hybrid warfare. This is because hybrid warfare can manifest in two main forms, either as a direct challenge to military forces or as a malign influence on civilian populations and decision-makers. This framework enables a systematic comparison of how different forms of hybrid warfare operate, depending on whether the principal focus is on controlling populations or defeating enemy forces.

Data has been collected from a diverse set of secondary sources, including books, peer-reviewed journal articles, think tank reports, governmental publications, and credible online materials. The findings and conclusions are drawn from the analysis of these empirical sources.

# 3. Case Studies

### *3.1. Russia's Annexation of Crimea (2014)*

In November 2013, then-Ukrainian President Viktor Yanukovych rejected signing the EU Association Agreement, opting instead to intensify his country's ties with Russia (Traynor and Grytsenko 2013). Yanukovych's decision to halt preparations for signing the agreement sparked widespread anti-government and pro-Western protests in the last month of the year, referred to as the "Euromaidan Revolution" (or the "Revolution of Dignity") (BBC News 2013). Though the Ukrainian government resorted to violence to crush the protests, the protesters eventually succeeded in ousting Yanukovych, and he fled to Russia on February 22, 2014 (DeBenedictis 2022, 11).

Crimea was and is of great geopolitical importance to Russia as the naval base in Sevastopol, which is located on the south-western coast of the peninsula, has been the main base of its Black Sea Fleet since the 18th century (Treisman 2016, 48). The Kremlin perceived the ousting of Ukraine's pro-Russian president Yanukovych as an illegal coup d'état orchestrated by Western powers (Kremlin 2014). In the eyes of the Kremlin, the overthrow of Yanukovych constituted a major challenge to Russia's national interests by endangering its access to its naval base in Sevastopol. For that reason, Moscow came to the decision to intervene covertly in Crimea. The strategic aim of the campaign was to reassert Russian sovereignty over the peninsula (BBC News 2015).

After the Verkhovna Rada (the Ukrainian parliament) voted to dismiss then-president Yanukovych from office, large-scale pro-Russian protests erupted in Crimea, where ethnic Russians and/or Russian speakers make up the largest demographic group (Gumuchian et al. 2017). The following day, pro-Russian protestors announced the formation of the self-styled "Crimean self-defense units" (Amos 2014). Yet, these street protests were widely believed to have been orchestrated by Russia's military and intelligence apparatus, including the GRU, the FSB, and the SVR, as well as Kremlin-backed paramilitary groups such as the Wagner Group and the Night Wolves (Bugriy 2014). In truth, during the Crimean operation, the so-called "self-defense units" essentially served as a *façade*, providing Russia-affiliated forces a local image (Bukkvoll 2016, 6).

Throughout the Crimean operation, soldiers wearing green uniforms without identifying markings, commonly known as "little green men", orchestrated and carried out separatist actions such as surrounding and assaulting military bases, demolishing military infrastructure, seizing key regional government administration buildings, in order to undermine Kyiv's sovereignty over the Peninsula (Galeotti 2019b, 5-12). Simultaneously, Russia steadily deployed reinforcements from its territory to Crimea to ensure operational success (Bartles and McDermott 2014, 58; Bukkvoll 2016, 17).

While the covert action to seize the Crimean Peninsula was accomplished within a couple of weeks, Moscow also employed several non-kinetic techniques to break Ukraine's determination to oppose its aggressive activities. It seems right to say that the key non-kinetic tool used by the Kremlin during the annexation of Crimea was psychological operations. The reason for this is that Russia's destabilizing propaganda activities tailored for Russians and Russian-speakers in the Crimean Peninsula seriously eroded the image of the newly formed Ukrainian government among the local population. The Kremlin's influence operations aimed to discredit the new government in Kyiv by portraying it as "fascists" and "Nazis", instill fear among pro-Russian population in the peninsula by implying that they were under serious threat from alleged "Ukrainian Nazis" and demonstrate widespread public support for Crimea's annexation by Russia (Kofman et al. 2017, 12-14; Treverton et al. 2018, 18; Bouwmeester, 2021, 505).

Amid skirmishes in Crimea between Russian-linked armed men and Ukrainian security forces, Russia reportedly conducted a series of cyber-attacks against Ukraine's computer networks and communications in March 2014. Russia aimed to divert public attention from Russian activities in and around the peninsula (Przetacznik and Tarpova 2022, 3). Another method worth mentioning is the use of coercive economic tools. Moscow imposed a temporary ban on Ukrainian pork imports on the grounds of inadequate veterinary oversight amid the country's instability. Simultaneously, the Russian Central Bank took control of Moscomprivatbank, which was owned by a Ukrainian oligarch, Ihor Kolomoyskyi, right after he criticized Russia's disruptive activities in Ukraine and accepted a government role in Dnipropetrovsk, an oblast located in eastern Ukraine. Furthermore, Moscow exerted diplomatic pressure to undermine the legitimacy of Ukraine's post-Maidan government. President Putin framed Euromaidan protests as an unconstitutional coup and subsequently declared the new authorities illegitimate (Kremlin 2014a).

Throughout the Crimean operation, the Russian government generated strategic ambiguity about both its methods and ultimate objectives. The armed groups involved in the disruptive activities could not be directly linked to the Russian state. As such, Moscow repeatedly denied any involvement in the pro-Russian uprising in Crimea. Throughout the Crimean operation, the Russian government generated strategic ambiguity about both its methods and ultimate objectives. The armed groups involved in the disruptive activities could not be directly linked to the Russian state. As such, Moscow repeatedly denied any involvement in the pro-Russian uprising in Crimea. In early March 2014, when "little green men" seized key government buildings in the Crimean Peninsula, President Putin, during a meeting with media representatives regarding the situation in Crimea, stated that "those were local self-defence units" in response to a question about the presence of Russian troops in the region (Kremlin 2014a). In the same meeting, when asked whether Russia would annex Crimea, he replied, "No, we do not." He further emphasized that only the Crimean people had the right to determine their own future (Kremlin 2014a).

Nonetheless, an independence referendum was held on March 16, 2014, in which the vast majority of Crimean voters reportedly supported joining Russia (Harding and Walker 2014). Subsequently, the Crimean parliament declared independence from Ukraine and requested to join Russia (BBC News 2014a). On March 18, despite widespread international condemnation, Russia annexed Crimea (MacAskill et al. 2014). The entire operation lasted just 26 days and remained largely bloodless. No significant armed confrontation occurred between Russian-affiliated forces and Ukrainian troops until March 18, when Russian-backed forces attacked a Ukrainian military outpost in Simferopol, resulting in the death of a Ukrainian officer (BBC News 2014b).

### *3.2. Russia's Covert Occupation of the Donbas Region*

The Donbas region of Eastern Ukraine, which is predominantly populated by ethnic Russians and Russian speakers, served as the political heartland of the pro-Kremlin President Viktor Yanukovych and his political party, the Party of the Regions. Thus, a significant portion of the population living in Donbas was profoundly dismayed by Yanukovych's ousting from power and felt anxious about Ukraine's political future (Kofman et al. 2017, 34; Galeotti 2019b, 14; Katchanovski 2016, 54).

Right after Ukraine's then-president Viktor Yanukovych was ousted, pro-Russian and anti-government protests took place across several oblasts in eastern Ukraine, most prominently in Donetsk, Luhansk, and Kharkiv (Salem 2014). Initially, pro-Russian activists were predominantly unarmed civilians (Kofman et al. 2017, 33-34). Their principal requests included a referendum on federalization, official recognition of Russian as a second state language, and the formation of a Customs Union with Russia (Trenin 2014, 7; Kofman et al. 2017, 36). However, these demonstrations were widely perceived as political theatre encouraged, if not orchestrated, by the Kremlin.

Throughout March 2014, Moscow incited and organized anti-government rallies across eastern Ukrainian cities (Roth 2014). However, at the time, pro-Russian protests remained relatively small in scale and largely non-violent (De Waal and Von Twickel 2020, 59). Although protestors briefly occupied administrative buildings, Ukraine's security forces were able to reassert control over them during the early phase of the political unrest in Donbas (Kofman et al., 2017, 38). Still, this initial tactical success failed to stem the deeper currents of political instability spreading across the region. The chaotic situation provided the Russian Federation with a great opportunity to intervene in the Donbas region in an indirect and covert manner.

Russia eroded Ukraine's sovereignty in Donbas by using similar instruments to those employed in Crimea. However, fighting in the separatist-held areas of the Donbas was violent and protracted. As seen in Crimea, "little green men" suddenly erupted. Russia deployed these unmarked soldiers to carry out clandestine military operations. These operations were orchestrated under the Kremlin's strategic leadership. However, they were executed through several agents involving tactical battalions, elite units such as

Spetsnaz, the Russian Airborne Troops (VDV), and the Special Operations Command (SOC), along with intelligence services, including the FSB and GRU. Moscow also conducted proxy warfare against Ukraine via armed non-state actors like the Wagner Group (Kofman et al., 2017). The most intense fighting in Donbas occurred between 2014 and 2015. While the situation appeared to stabilize somewhat in the following years, hostilities never fully ceased. Between 2014 and 2022, the war in Donbas claimed more than 14,000 lives (International Crises Group, n.d.). The conflict between Ukrainian security forces and Russian-affiliated groups continued until February 24, 2022, when the Kremlin escalated its prolonged and violent hybrid warfare operation into a direct force-on-force confrontation.

As part of its prolonged hybrid warfare campaign in Donbas, alongside military measures, Russia significantly benefited from a wide range of non-military instruments to decrease the necessity for employing military force to a minimum level. Offensive cyberspace operations were of notable importance. Starting in 2014, Russia carried out several cyber-attacks to disrupt Ukraine's network infrastructure. Ukraine power grid hack (2015), paralysis of the State Treasury of Ukraine (2016), and Ukraine ransomware attacks (2017) were just a few examples of cyber-attacks carried out by Russian-affiliated groups (Przetacznik and Tarpova 2022).

Another important component of Russia's hybrid warfare campaign was propaganda. Russia conducted sophisticated propaganda activities to provoke ethnic Russians in Ukraine, demonize Ukrainian armed forces, influence the attitudes of the conflict zone population, and spread its narrative to the global audience via various media and internet platforms (Yuhas 2014). Russia also exerted economic coercion to destabilize Ukraine. For instance, in June 2014, Moscow cut off gas supplies to Ukraine as the armed conflict between Ukrainian forces and pro-Russian insurgents in the Donbas region intensified and subsequently threatened to do it again (BBC 2014c).

As exemplified during the annexation of Crimea, the Kremlin employed the strategy of plausible deniability in the war in Donbas as well. Although Ukraine accused Moscow of provoking or even directly participating in the armed conflict in the Donbas region, Russian authorities repeatedly denied any involvement. For example, in April 2014, Putin stated:

> Nonsense. There are no Russian units in eastern Ukraine – no special services, no tactical advisors. All this is being done by the local residents, and the proof of that is the fact that those people have literally removed their masks (Kremlin 2014b).

Likewise, Russia's Foreign Minister Sergey Lavrov claimed that there was no proof of Russia deploying its armed forces in the war in Donbas (Baczynska 2015). While addressing viewers in a live television program in April 2015, President Putin said: On the question whether or not our military is in Ukraine, I am telling you directly and clearly: there are no Russian troops (Kremlin 2015).

Yet, in the ensuing months, Russia subtly shifted its stance on its involvement in the war in Donbas. In late 2015, President Putin acknowledged that Russia's special operation forces were active in the region, stating, "We never said there were no people there who carried out certain tasks, including in the military sphere". Nevertheless, he highlighted that it was different from Russia's regular army (Walker 2015). Putin's remarks about Russia's role in the Donbas conflict were superficial and offered little insight into the activities of Russia's armed forces in the region. Therefore, despite overwhelming evidence to the contrary, it remains accurate to say that Russia maintained a level of plausible deniability during the Donbas operation.

## 4. Findings

Research findings suggest that the Russian annexation of Crimea and covert occupation of the Donbas region indicate two different types of hybrid warfare. Despite the existence of heavily armed groups, colloquially called little green men, in taking control of administrative buildings and critical sites in Crimea, the Crimean operation was almost bloodless. In 2014, when Kremlin-affiliated forces seized control of Crimea, cognitive operations played a central role in influencing popular sentiment and discrediting the Ukrainian administration. These methods sought to strengthen control over Crimeans, especially ethnic Russians and/or Russian speakers, coerce Ukrainian officials, and instill fear among Ukraine's pro-Western communities, primarily residing in the western and northern regions of the country. Moreover, other non-military tools, including cyber-attacks, diplomatic pressure, and economic coercion, played a role in Russia's hybrid warfare campaign in Crimea. The Russian Federation weakened or even destroyed Ukraine's control over Donbas by using the same instruments; however, the conflict was far more intense and protracted than the operation in Crimea.

As previously noted, David Kilcullen's concepts of population-centric and enemy-centric approaches may offer insight into the different forms of hybrid warfare. He draws a distinction between two models: the population-centric approach focuses on winning control over the people and their surroundings, on the assumption that once that is achieved, other goals will fall into place. The enemy-centric approach, by contrast, treats counterinsurgency more like conventional warfare, aiming first and foremost to defeat the enemy, in the belief that everything else will follow once that happens.

Relying on Kilcullen's (2007) model, hybrid warfare can be classified into two sub-categories based on the nature of the actions (disruptive vs. destructive) and their primary targets: population-centric hybrid warfare and enemy-centric hybrid warfare. This distinction stems from the fact that the hybrid model of warfare can be conducted in two principal modes, either as an intense and direct challenge to the enemy's armed forces or as a malign influence campaign on the enemy's civilian population and key political decision-makers. It appears suitable to assert that

Russia's seizure of the Crimean Peninsula is more in line with population-centric hybrid warfare, as it primarily aims to control the population and sway enemy policymakers with minimal use of force. Conversely, Russia's covert occupation of the Donbas region typifies enemy-centric hybrid warfare. The reason for this is that the principal objective of the Donbas operation was essentially the military defeat of Ukrainian forces. It is worth emphasizing that many features of the Donbas operation overlap with those of the Crimean operation. Namely, despite the use of high-intensity violence, Russia also sought to establish control over the conflict-zone population and influence enemy decision-makers during the Donbas operation. However, the strategic logic differed: in Donbas, the priority was direct confrontation and operational victory over the enemy. The comparison between the Crimean operation and the Donbas operations is shown in Table 1 below.

**TABLE NO. 1**
**Crimean Operation vs Donbas Operation**

| | **Crimean Operation** | **Donbas Operation** |
|---|---|---|
| **Objectives** | Intimidation of Ukraine's political decision-making and mobilisation of Russian-speaking communities in the Crimean Peninsula | Wearing down Ukraine's military forces in Donbas and seizing critical areas |
| **Methods** | Activities that do not include direct physical force | Integration of covert/indirect military force with non-military tools |
| **Targets** | Ukraine's population and decision-makers | Ukraine's population, decision-makers, and military |

## Conclusion

While hybrid warfare, both as a concept and an actual mode of warfare, includes a wide variety of unfriendly behaviors, its broad definition has often led to analytical ambiguity. This article has proposed a new taxonomy of hybrid warfare by distinguishing between Russia's operations in Crimea and Donbas, which are colloquially seen as the defining examples of the hybrid model of warfare. The comparative analysis of Russia's operations in Crimea and the Donbas suggests that hybrid warfare can be operationalized in two different forms, despite sharing a common strategic logic of staying below the threshold of conventional warfare. Thus, by drawing on David Kilcullen's counterinsurgency framework, the article introduces a distinction between population-centric hybrid warfare and enemy-centric hybrid warfare. The former focuses on shaping perceptions and gaining the support or acquiescence of local populations, whereas the latter aims at defeating adversary forces. Russia's annexation of Crimea illustrates a population-centric hybrid warfare model, given that the primary aim was controlling the Crimean population and

influencing key decision-makers. In contrast, Russia's covert occupation of Donbas aligns with an enemy-centric hybrid warfare model because it involved actual fighting and bloodshed. This typological framework enhances conceptual clarity and provides a useful lens for analyzing diverse hybrid warfare campaigns. This article tries to take the first step in categorizing varied forms of hybrid warfare. Accordingly, it does not assert that it provides conclusive results. Therefore, it invites further research into other hybrid warfare campaigns by applying the proposed taxonomy to them.

## References

**Amos, Howard.** 2014. "Ukraine Crisis Fuels Secession Calls in pro-Russian South." The Guardian. https://www.theguardian.com/world/2014/feb/23/ukraine-crisis-secession-russian-crimea.

**Baczynska, Gabriela.** 2015. "Russia Says no Proof it Sent Troops, Arms to East Ukraine." Reuters. https://www.reuters.com/article/world/russia-says-no-proof-it-sent-troops-arms-to-east-ukraine-idUSKBN0KU14I/.

**Bartles, Charles K., and Roger N. McDermott.** 2014. "Russia's Military Operation in Crimea: Road-Testing Rapid Reaction Capabilities." Problems of Post-Communism 61 (no. 6): 46–63. doi:10.2753/PPC1075-8216610604.

**BBC News.** 2013. "Ukraine Protests: Singing in the Cold." https://www.bbc.com/news/world-europe-25468055.

**___.** 2014a. "Crimean Parliament Formally Applies to Join Russia." https://www.bbc.com/news/world-europe-26609667.

**___.** 2014b. "Ukraine Officer 'killed in Attack on Crimea Base." https://www.bbc.com/news/world-europe-26637296.

**___.** 2014c "Ukraine Crisis: Russia Halts Gas Supplies to Kiev." https://www.bbc.com/news/world-europe-27862849.

**___.** 2015. "Putin Reveals Secrets of Russia's Crimea Takeover Plot." https://www.bbc.com/news/world-europe-31796226.

**Bērziņš, Jānis.** 2019. "Not 'Hybrid' but New Generation Warfare." In Russia's Military Strategy and Doctrine, edited by Glen E. Howard and Matthew Czekaj. Washington, DC: The Jamestown Foundation.

**Bouwmeester, Han.** 2021. The Art of Deception Revisited (Part 2): The Unexpected Annexation of Crimea in 2014. Militaire Spectator, 190 (no. 10): 494-507. https://militairespectator.nl/artikelen/art-deception-revisited-part-2-unexpected-annexation-crimea-2014.

**Bugriy, Maksym.** 2014. The Crimean operation: Russian Force and Tactics. Eurasia Daily Monitor, 11 (no. 61). https://jamestown.org/program/the-crimean-operation-russian-force-and-tactics/.

**Bukkvoll, Tor.** 2016. "Russian Special Operations Forces in Crimea and Donbas." Parameters 46, (no. 2). doi:10.55540/0031-1723.2917.

**Connell, M. Ellen and Ryan Evans.** 2015. Russia's "Ambiguous Warfare" and Implications for the U.S. Marine Corps. Arlington, VA: CNA Analysis & Solutions.

**Dalton, Melissa G.** 2017. "How Iran's Hybrid-War Tactics Help and Hurt It." Bulletin of the Atomic Scientists 73 (no. 5): 312–15. https://doi.org/10.1080/00963402.2017.1362904.

**DeBenedictis, Kent.** 2022. Russian 'Hybrid Warfare' and the Annexation of Crimea: The Modern Application of Soviet Political Warfare. London: I.B. Tauris.

**De Waal, Thomas and Nikolaus Von Twickel.** 2020. Beyond Frozen Conflict: Scenarios for the Separatist Disputes of Eastern Europe. London: Rowman & Littlefield International.

**European Commission.** 2016. Joint Communication- Joint Framework on Countering Hybrid Threats JOIN (2016) 18 final. Brussels: European Union.

**Freedman, Lawrence.** 2014. "Ukraine and the Art of Limited War." Survival 56 (no. 6): 7–38. https://doi.org/10.1080/00396338.2014.985432.

**Galeotti, Mark.** 2019a. Russian Political War: Moving Beyond the Hybrid. Abingdon: Routledge.

**___.** 2019b. Armies of Russia's war in Ukraine. Oxford: Osprey Publishing.

**Gumuchian, Marie-Louise, Laura Smith-Spark, and Ingrid Formanek.** 2014. "Gunmen Seize Government Buildings in Ukraine's Crimea, Raise Russian Flag." https://edition.cnn.com/2014/02/27/world/europe/ukraine-politics/index.html.

**Harding, Luke, and Shaun Walker.** 2014. "Crimea Votes to Secede From Ukraine in 'İllegal' Poll." The Guardian. https://www.theguardian.com/world/2014/mar/16/ukraine-russia-truce-crimea-referendum.

**Hoffman, Frank G.** 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies. https://potomacinstitute.us/reports/19-reports/1163-conflict-in-the-21st-century-the-rise-of-hybrid-wars.

**International Crises Group.** n.d. Conflict in Ukraine's Donbas: A Visual Explainer. https://www.crisisgroup.org/content/conflict-ukraines-donbas-visual-explainer.

**Kang, Deasu.** 2020. The Multi-Domain Operation's Viability as a Future War Concept of the Republic of Korea Military: Can It Counter North Korean Hybrid Warfare? Fort Leavenworth, Kansas: U.S. Army Command and General Staff College. https://apps.dtic.mil/sti/pdfs/AD1124669.pdf.

**Katchanovski, Ivan.** 2016. "The Separatist War in Donbas: A Violent Break-up of Ukraine?" European Politics and Society 17 (no. 4): 473–89. https://doi.org/10.1080/23745118.2016.1154131.

**Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer.** 2017. Lessons from Russia's Operations in Crimea and Eastern Ukraine. Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RR1498.html

**Kilcullen, David.** 2007. "Two Schools of Classical Counterinsurgency." Small Wars Journal, January 28, 2007. https://smallwarsjournal.com/2007/01/28/two-schools-of-classical-counterinsurgency/.

___. 2020. The Dragons and the Snakes: How the Rest Learned to Fight the West. Oxford: Oxford University Press.

**Kremlin.** 2014a. "Vladimir Putin Answered Journalists' Questions on the Situation in Ukraine." http://en.kremlin.ru/events/president/news/20366.

**___.** 2014b. Direct Line with Vladimir Putin." http://en.kremlin.ru/events/president/news/20796.

**Libiseller, Chiara.** 2023. "'Hybrid Warfare' as an Academic Fashion." Journal of Strategic Studies 46 (no. 4): 858–80. https://doi.org/10.1080/01402390.2023.2177987.

**Mazarr, Michael, J.** 2015. Mastering the Gray Zone: Understanding a Changing Era of Conflict. Carlisle, PA: US Army War College Press. https://press.armywarcollege.edu/monographs/428.

**MacAskill, Ewen, Shaun Walker, and Dan Roberts.** 2017. "Ukraine: Putin Approves Draft Bill for Russia to Annex Crimea." The Guardian. https://www.theguardian.com/world/2014/mar/18/ukraine-putin-draft-bill-russia-annex-crimea.

**Miracola, Sergio.** 2018. Chinese Hybrid Warfare. Italian Institute for International Studies. https://www.ispionline.it/en/publication/chinese-hybrid-warfare-21853.

**Mockaitis, Thomas R.** 1990. British Counterinsurgency, 1919–60. London: Palgrave Macmillan.

**Mumford, Andrew, and Pascal Carlucci.** 2023. "Hybrid Warfare: The Continuation of Ambiguity by Other Means." European Journal of International Security 8 (no.2): 192–206. https://doi.org/10.1017/eis.2022.19.

**NATO.** 2014. "Wales Summit Declaration Issued by NATO Heads of State and Government." https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

**___.** 2024. "Countering Hybrid Threats." https://www.nato.int/cps/en/natohq/topics_156338.htm.

**Popescu, Nicu.** 2015. "Hybrid Tactics: Neither New nor Only Russian." European Union Institute for Security Studies Issue Alert 4: 1-2. https://www.iss.europa.eu/publications/alerts/hybrid-tactics-neither-new-nor-only-russian.

**Przetacznik, Jakub, and Tarpova Simona.** 2022. Russia's War on Ukraine: Timeline of Cyber-Attack. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

**Radin, Andrew, Alyssa Demus, and Krystyna Marcinek.** 2020. "Understanding Russian Subversion: Patterns, Threats, and Responses." Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/perspectives/PE331.html.

**Rasmussen, Anders Fogh.** 2014. Future NATO. Speech by NATO Secretary General Anders Fogh Rasmussen at Chatham House - London, United Kingdom. https://www.nato.int/cps/en/natolive/opinions_111132.htm.

**Roth, Andrew**. 2014. "From Russia, 'Tourists' Stir the Protests. The New York Times." The New York Times. https://www.nytimes.com/2014/03/04/world/europe/russias-hand-can-be-seen-in-the-protests.html.

**Salem, Harriet.** 2017. "Deep Divisions Split Donetsk as Tensions Simmer Across Ukraine." The Guardian. https://www.theguardian.com/world/2014/mar/04/ukraine-russia-protesters-donetsk-separate-by-force.

**Traynor, Ian, and Oksana Grytsenko.** 2013. "Ukraine Suspends Talks on EU Trade Pact as Putin Wins Tug of War." The Guardian. https://www.theguardian.com/world/2013/nov/21/ukraine-suspends-preparations-eu-trade-pact.

**Treisman, Daniel.** 2016. "Why Putin Took Crimea: The Gambler in the Kremlin." Foreign Affairs 95 (no. 3): 47–54. http://www.jstor.org/stable/43946857.

**Trenin, Dimitri.** 2014. The Ukraine Crises and the Resumption of Great-Power Rivalry. Moscow: Carnegie Moscow Center.

**Treverton, Gregory F., Andrew Thvedt, Alicia R. Chen, Kathy Lee, and Madeline McCue.** 2018. Addressing Hybrid Threats. Stockholm: Swedish Defence University.

**Yuhas, Alan.** 2017. "Russian Propaganda Over Crimea and the Ukraine: How Does It Work?" The Guardian. https://www.theguardian.com/world/2014/mar/17/crimea-crisis-russia-propaganda-media.

**Walker, Shaun.** 2015. "Putin Admits Russian Military Presence in Ukraine for First Time." The Guardian. https://www.theguardian.com/world/2015/dec/17/vladimir-putin-admits-russian-military-presence-ukraine.

**Wither, James K.** 2016. "Making Sense of Hybrid Warfare." Connections the Quarterly Journal 15 (no. 2): 73–87. http://dx.doi.org/10.11610/Connections.15.2.06.

**Conflict of Interest Statement**

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

**Funding Information**

This article draws on data gathered as part of my doctoral research conducted at the Strategy and Security Institute, University of Exeter. The research is produced under the scholarship provided by the Turkish Ministry of National Education.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Security Expenditures and Fiscal Strain: The Impact of the Farmer-Herder Conflict on Public Finance in Northern Nigeria (2015-2024)

**Ibrahim O. SALAWU, PhD***
**Moshood Olayinka SALAHU, PhD****
**Emmanuel Oyewole LAMBE, PhD*****
**Hassan Seyid ISHOLA, PhD******

*Department of Politics and Governance, Kwara State University, Malete
e-mail: ibrahimsalus@gmail.com
**Department of Politics and Governance, Kwara State University, Malete
e-mail: moshoodsalahu@gmail.com
***Department of Politics and Governance, Kwara State University, Malete
e-mail: Emmanuel.lambe60@gmail.com
****Department of Politics and Governance, Kwara State University, Malete
e-mail: Hassancisse1616@gmail.com

## Abstract

Nigeria has been entrapped in a cycle of insecurity which has not only affected the lives and properties of its citizens, but as had a colossal effect on the macro-economy of the state. The waves of insecurity since the genesis of the fourth republic have created patterns of unending micro and macro insecurity, with a resounding feature of immediate and relative financial consequences. This insecurity in multiple parts of the Northern part of Nigeria broadens and stretches the state's efforts to thwart the violence. So, this study examines the fiscal implications of insecurity on Nigeria's public finance between 2015 and 2024, with a focus on defence expenditure, social sector allocations, and revenue generation. Using panel data and the systems theory framework, the research explores how escalating insecurity driven by insurgency, banditry, and herder-farmer conflicts has shifted fiscal priorities towards defence spending at the expense of critical sectors like education, health, and agriculture. Empirical findings reveal that insecurity has led to a disproportionate allocation of resources to defence, rising from $16 billion in cumulative spending between 2008 and 2018 to N3.25 trillion in 2024 alone, representing 12% of the national budget. Concurrently, revenue generation has declined due to disruptions in agricultural production, trade, and investment in conflict-prone areas, thereby constraining fiscal space. Comparative insights from conflict-affected countries such as Afghanistan and Somalia further illustrate the destabilising economic effects of prolonged insecurity.

**Keywords:**
insecurity; public finance; expenditure; political system; military.

**Article info**
Received: 6 April 2025; Revised: 30 April 2025; Accepted: 16 May 2025; Available online: 27 June 2025

Citation: Salawu, I.O., M.O. Salahu, E.O. Lambe, and H.S. Ishola. 2025. "Security Expenditures and Fiscal Strain: The Impact of the Farmer-Herder Conflict on Public Finance in Northern Nigeria (2015–2024)." *Bulletin of "Carol I" National Defence University*, 14(2): 62-81. https://doi.org/10.53477/2284-9378-25-16

## 1. Introduction

Globally, fiscal structures have witnessed significant transformations due to shifting global economic demands, especially in the wake of the COVID-19 pandemic, and the Russia-Ukraine war, which triggered unprecedented economic disruptions (Rezai, et al. 2024). As governments scrambled to address public health crises, social welfare challenges, and economic recovery, fiscal deficits widened substantially. At the same time, rising insecurity has driven many countries to divert resources from development expenditures toward military spending. The Stockholm International Peace Research Institute (SIPRI 2023) highlights that global military expenditures rose to over $2 trillion by 2022, reflecting increased insecurity and increased defence allocations across nations grappling with geopolitical tensions, domestic insecurity, and post-pandemic recovery deficits. This phenomenon has been especially pronounced in low- and middle-income countries such as South Sudan, Algeria, DRC, Mexico, Ukraine, and Poland, where the fiscal strain has translated into reduced investments in sectors essential for long-term socio-economic development, including education, health, and agriculture.

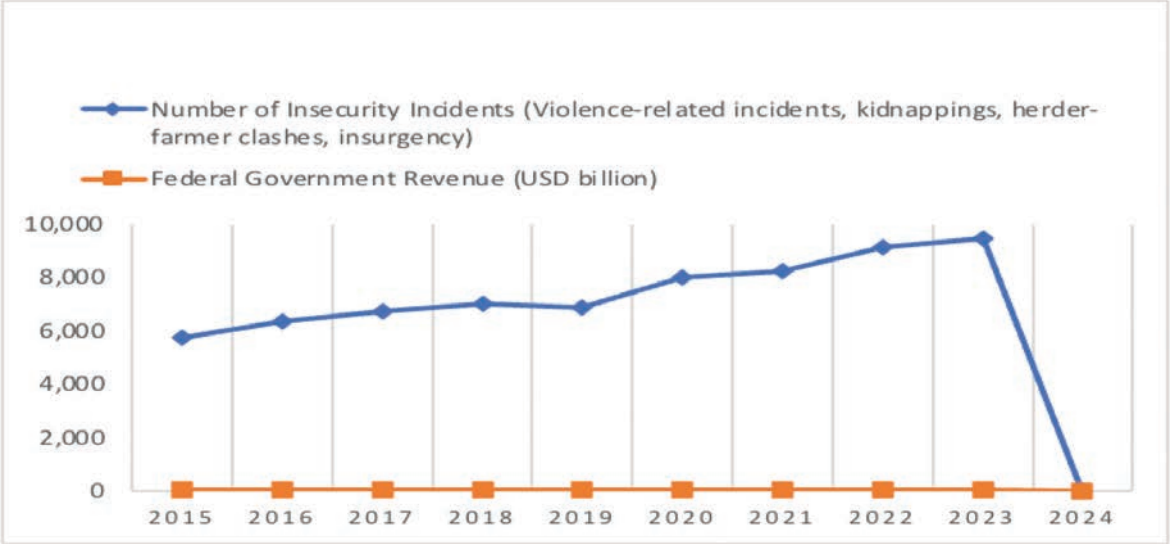
On the African continent, fiscal pressures have intensified due to chronic instability, particularly in the Sahel, where weak state structures, transnational terrorism, and organised crime have exacerbated a new market for insecurity. The porous borders of the Sahel region have facilitated the proliferation of small arms, human trafficking, and the movement of extremist groups, creating a complex, multi-dimensional security crisis. The Multinational Joint Task Force (MNJTF 2021) reports that insecurity in the Sahel has displaced over five million people and cost affected economies more than $30 billion annually in lost productivity, disrupted trade, and damaged infrastructure. This instability has been partly linked to the destabilising ripple effects of the Arab Spring, which, since 2011, created security vacuums in Libya and other North African states, enabling the spread of jihadist insurgencies and illicit arms networks into West Africa. These dynamics have amplified fiscal vulnerabilities in affected countries, where rising defence budgets have crowded out investments in health, education, and social services.

Over the last decade, Nigeria's fiscal capacity has sharply declined (Aganga 2023), therefore undermining the state's ability to fund core developmental functions. Between 2014 and 2016, the collapse in global oil prices on which Nigeria depended for over 70% of government revenue fell, which resulted in significant shortfalls in the government's spending and ability to manage the country's fiscal responsibility. With oil revenue dropping from ₦6.8 trillion in 2014 to ₦1.9 trillion by 2016 (CBN 2017) and also compounded by persistent insecurity that disrupted non-oil revenue sources, especially agriculture and trade in the North, the state's capacity to raise and allocate resources for public services weakened drastically.
In northern Nigeria, where this insecurity was predominant, the waves of insecurity have reached unprecedented levels since 2015 due to the simultaneous rise of Boko

Haram insurgency, herder-farmer clashes, Unknown Gunmen (UGM) and banditry. According to the Global Terrorism Index by the institute for economic and peace (IEP 2022), Nigeria consistently ranks among the top ten countries most affected by terrorism, with thousands of lives lost annually and millions displaced. This insecurity has necessitated a dramatic increase in military spending, with Nigeria's defence budget more than tripling between 2015 and 2024. By 2022, defence allocations reached approximately ₦2.5 trillion, representing over 15% of total federal spending (Budget Office of the Federation 2022). However, this increased security expenditure has coincided with stagnation in key social sectors. Allocations to education and health, for instance, remain below UNESCO and WHO recommendations, limiting progress in human capital development. The insecurity itself has also disrupted economic activity, particularly in northern Nigeria's agrarian communities, where banditry and insurgency have displaced farmers, reduced agricultural output, and contracted the government's tax base. This cyclical dynamic, where insecurity worsens fiscal capacity and reduced fiscal capacity exacerbates insecurity and has left Nigeria facing protracted fiscal instability, with implications for broader development goals.

Nigeria's persistent insecurity, particularly in the northern region, has profoundly reshaped its fiscal landscape over the past decade. With an estimated 80,000 deaths attributed to insurgency, banditry, and herder-farmer clashes between 2015 and 2024 (ACLED 2024), the country's security crisis has escalated into a multi-front war that continues to exact a heavy toll on lives, livelihoods, and public finances. This protracted conflict has forced the Nigerian government to allocate an increasingly disproportionate share of its budget to defence and security. For instance, defence spending rose by over 280%, from ₦504 billion in 2015 to ₦3.25 trillion in 2024 (Statista 2024) at the expense of investments in key developmental sectors like education and health.

**Graph 1** Trend of macro-insecurity incidents in Northern Nigeria (2015-2024)




**Source:** Researchers' survey, across NBS, CBN, Nigeria Security Tracker, IMF

The fiscal impact of this security crisis is evident in the declining allocations to social sectors. Despite Nigeria's growing population and worsening human development indicators, the education sector's share of the national budget stagnated at around 5–7% annually, far below the UNESCO-recommended benchmark of 15–20%. Similarly, health sector allocations, though increasing in nominal terms, have remained insufficient to meet the country's worsening health outcomes, as seen in Nigeria's high maternal mortality ratio of 512 per 100,000 live births (World Bank 2023). This imbalance has hindered efforts to improve infrastructure, recruit and retain skilled personnel, and enhance service delivery, further deepening Nigeria's development challenges.

The pervasive insecurity has also disrupted economic activities, particularly in agriculture, a key sector in northern Nigeria. The Food and Agriculture Organisation (FAO) estimates that herder-farmer conflicts alone have cost the Nigerian economy over $14 billion annually due to lost agricultural output, displacement, and destroyed farmlands. This disruption, combined with deteriorating business confidence, has contracted the tax base and reduced government revenues. Consequently, Nigeria's fiscal deficit has widened, necessitating increased borrowing and exacerbating the debt crisis. By 2024, debt servicing alone accounted for 74% of total federal revenues, leaving minimal fiscal space for developmental priorities.

Moreover, the inflationary pressures driven by insecurity-related supply chain disruptions have worsened the economic hardship for ordinary Nigerians. The inflation rate surged from 9% in 2015 to over 24% in 2023, eroding purchasing power and exacerbating poverty, particularly in the conflict-affected northern region. This cyclical insecurity-fiscal strain nexus has trapped Nigeria in a state of perpetual instability, where insecurity depletes fiscal resources, weakens socio-economic resilience, and perpetuates the very conditions that fuel further unrest. In lieu of this, the study examines the fiscal implications of this insecurity from 2015 to 2024, analysing how government expenditure patterns have evolved in response to these persistent threats.

## 2. Research methodology

This research employs a mixed-methods design, integrating quantitative analysis of panel data with secondary qualitative insights to explore the fiscal consequences of insecurity in Northern Nigeria between 2015 and 2024. By adopting a time series and longitudinal approach, the study examines trends in budgetary allocations to key sectors, including defence, health, education, and agriculture, while examining macroeconomic variables such as debt servicing, inflation, and oil revenues. The data, drawn from reputable institutions like the Budget Office of the Federation, Central Bank of Nigeria, World Bank, and Global Terrorism Index, undergo statistical scrutiny through descriptive and inferential techniques, with an emphasis on trend

analysis and panel regression. The research applies the system theory to interpret the fiscal trade-offs arising from prolonged insecurity. To enhance reliability and validity, the study employs triangulation and diagnostic tests of autocorrelation, ensuring robust findings and ethical adherence through accurate sourcing and representation of data.

## 3. Literature Review

### 3.1. Concept of Insecurity

Insecurity is the state of vulnerability to injury, danger, or threat, be it physical, economic, or social. It entails a lack of safety, stability, or defence against violence and harm. Scholars and institutions have defined insecurity in various ways, and much of the literature highlights its multidimensionality. Wolfers (1952) posits insecurity as the absence of physical and psychological stability, while Collier and Hoeffler (2004) emphasise political instability, civil war, and bad governance as causes of insecurity, particularly in fragile states. Insecurity could be categorised into forms like physical insecurity (which includes violence, terrorism, insurgency, and armed conflict), food insecurity, economic insecurity, and cyber insecurity. In the Nigerian situation, insurgency, banditry, herder-farmer conflicts, and kidnapping are the most prevalent forms of insecurity. These security challenges have been particularly atrocious in Northern Nigeria, where instability has resulted in the loss of lives and property, the displacement of the people, and the disruption of agricultural production and trade. The insecurity in Northern Nigeria is also heightened by the permeable borders of the Sahel, transnational organised crime, institutional capacity shortfall, and a history of resource-based violence in the past. The pervasive insecurity has broader socio-economic implications because it affects governance, reduces foreign and domestic investment, and increases public spending on security and defence at the detriment of other relevant sectors like education, health, and infrastructure. Scholars such as Ake (1996) argue that insecurity also undermines democratic governance and state legitimacy as citizens lose faith in the ability of the state to protect lives and property. Insecurity, therefore, is not just a security issue but a systemic one that impacts public policy, fiscal management, and overall socio-political stability.

To incorporate the dataset effectively into the section 3.2 Concept of Public Finance, you should use it to empirically support the paragraph that discusses the weakening fiscal position of the Nigerian state due to insecurity and external shocks. The integration should serve as an evidentiary bridge between theoretical public finance and the actual fiscal trajectory of Nigeria.

### 3.2. Concept of Public Finance

Public finance is the study of how the government raises revenue, distributes resources, and controls spending in order to attain economic stability, equity, and efficiency. Public finance is concerned with the state's fiscal function, taxation, borrowing, government expenditure, and management of fiscal policy. Musgrave (1989) define public finance as having three key functions:

1. Allocation Function – The provision of efficient public goods and services.
2. Distribution Function – Redistributing income and wealth to promote social equality.
3. Stabilisation Function – Use of fiscal tools to confer macroeconomic stability, including controlling inflation, reducing unemployment, and stabilising economic growth.

In Nigeria, public finance has historically been dominated by oil revenue, accounting for the majority of government income. However, since 2015, this dependency has become a critical vulnerability due to global oil price volatility, domestic oil theft, corruption, and disruptions from insecurity. Between 2015 and 2024, government revenue as a percentage of GDP oscillated widely, dropping as low as 5.1% in 2016 during the oil price crash and pandemic aftermath, before climbing to a projected 12.4% by 2024 following structural reforms and subsidy removals (IMF 2023; Oxford Business Group 2024).

| *Year* | **Govt Revenue (% of GDP)** | **Oil Revenue (% of GDP)** | **Non-Oil Revenue (% of GDP)** |
|---|---|---|---|
| *2015* | 7.5% | 3.2% | 4.3% |
| *2016* | 5.1% | 2.2% | 2.9% |
| *2017* | 6.6% | 2.5% | 4.1% |
| *2018* | 8.5% | 3.0% | 5.5% |
| *2019* | 7.8% | 2.8% | 5.0% |
| *2020* | 6.5% | 2.4% | 4.1% |
| *2021* | 7.1% | 2.3% | 4.8% |
| *2022* | 9.0% | 3.6% | 5.4% |
| *2023* | 9.4% | 2.9% | 6.5% |
| *2024* | 12.4% (proj.) | 6.0% (proj.) | 6.5% (proj.) |

This fiscal contraction was exacerbated by increased security expenditures, which crowded out critical sectors such as education and health. The post-2020 period particularly reflects the compound effects of the COVID-19 pandemic, the global energy crisis stemming from the Russia-Ukraine war, and major structural reforms initiated in 2023 by the new administration. These events not only impaired oil exports and disrupted non-oil sectors but also widened the fiscal deficit and triggered debt-servicing pressures. As a result, Nigeria's capacity to fulfil the Musgravian functions of public finance has been severely constrained, especially in stabilising the macroeconomy and delivering equitable services.

**3.3. Theoretical Framework:**

***Systems Theory***

The Systems Theory, formulated based on the works of Ludwig von Bertalanffy in the 1950 but it is majorly attributed and influenced by Easton (1971). He views the state as an interdependent and dynamic system composed of various interdependent

subsystems such as security, economy, education, health, and public finance. The subsystems work together for the stability and viability of the overall system (the state). When one of the subsystems, say security, experiences long-term instability or malfunction, it has a chain effect that destabilises other subsystems, weakening the balance of the overall structure. Further, David Easton's political system theory enriches this debate inasmuch as it imagines the state as a dynamic system processing inputs (for instance, demands for security) and producing outputs (for instance, policy and budgetary allocations). Easton's input-output model helps to explain how the chronic insecurity in the north generates fiscal pressures that lead to skewed defence expenditures while reducing investments in socio-economic infrastructure. The continuous feedback process of violence and instability feeds back into the system, elongating its overall equilibrium and affecting governance, resource distribution, and long-term development.

In the example of Northern Nigeria's insecurity (2015–2024), the persistent waves of insurgency, banditry, and herder-farmer conflicts represent a core failure in the security subsystem. The failure disrupts the normal socio-economic operations, leading to low agricultural output, economic displacement, and infrastructural damage. As a result, the Nigerian government is forced to allocate disproportionately large resources to the defence sector to manage this security crisis at the expense of key sectors like health, education, and agriculture. This reallocation, however, produces negative "outputs" like decreased investment in human capital development, higher debt servicing, and undermined social services, which further destabilise the socio-economic system. The financial burden occasioned by insecurity thus weakens the capacity of the state to provide essential services, which worsens poverty, inequality, and governance problems, thereby fuelling a vicious cycle of systemic instability.

***Applications of the theory***

Applying Systems Theory, the research conceptualises insecurity not as an isolated phenomenon but as part of an overall systemic breakdown with rippling effects on public finance and national development. The theory calls for restoring equilibrium to the state system by addressing the root causes of insecurity.

### 3.4. Historical Overview of Insecurity in the Nigeria Fourth Republic

***Insurgency: The Boko Haram Threat (2015–2024)***

The Boko Haram insurgency, which started in the early 2000s, has remained a significant threat to peace and stability in Northern Nigeria, particularly in the Northeast. Despite intensified military operations, including the deployment of Operation Lafiya Dole in 2015 and ongoing counterinsurgency operations aided by regional forces like the Multinational Joint Task Force (MNJTF), Boko Haram and its splinter group, the Islamic State West Africa Province (ISWAP), have maintained the capacity to carry out attacks. These come in the shape of bombings, kidnappings, and attacks on military bases and civilian villages. As of 2022, the United Nations High Commissioner for Refugees (UNHCR) put the number of people internally

displaced due to the insurgency at over 2.2 million, with Borno State being the most impacted (UNHCR 2022). The economic implications have been catastrophic, with defence expenditures rising steadily to counter the insurgency, while humanitarian needs, such as food support and education for displaced children, have strained government resources.

***Banditry in the Northwest***

Since 2016, banditry has emerged as one of the most pressing security challenges in the Northwestern states, particularly Zamfara, Katsina, Sokoto, and Kaduna. What was initially considered small-scale local criminality in the guise of cattle rustling has escalated into a more organised and brutal conflict, with armed fighters committing widespread kidnappings for ransom, mass atrocities, and village burnings. Between 2021 and 2019, over 1,600 people were killed by bandits in Katsina and Zamfara, and thousands of others left displaced, according to a report by United Nations High Commissioner for Refugees (UNHCR) and Nigeria's National Commission for Refugees, Migrants, and Internally Displaced Persons (NCFRMI) (IEP 2022). The simplicity of movement across the porous borders between Nigeria and Niger has facilitated the flow of small arms, worsening the violence and making it difficult to conduct counter-banditry operations. The government has responded in the center by increasing military deployments and declaring a no-fly zone over Zamfara State in 2021 to stop illegal mining and arms trafficking. Nevertheless, the persistence of banditry has been socio-economically devastating, affecting agriculture (one of the main livelihood in the region) and local government revenue due to rural population displacement and the disruption of market activities.

***Herder-Farmer Conflicts in North Central Nigeria***

The herder-farmer conflict, primarily affecting Benue, Plateau, Nasarawa, and Taraba States, has deep historical roots linked to competition over land and water resources. However, climate change, population growth, and the southward migration of nomadic herders from the Sahel have intensified these clashes over the past decade. Between 2015 and 2020, over 8,000 people died, and hundreds of communities were displaced from their homes due to clashes, according to the International Crisis Group (2021). These have escalated ethnic and religious tensions, most significantly in Benue and Plateau States, where farmers (predominantly Christian communities) and herders (largely Fulbe Muslims) accuse each other of violence and encroachment on resources. Federal and state government interventions in ending the hostilities, as in the example of passing anti-open grazing policies in Benue and Ekiti States, have been received with mixed success, with observers criticising such regulations for the tendency to heighten tensions by circumscribing pastoral livelihoods while not providing pragmatically functional alternatives. This has resulted in the following instability undermining agricultural production in the region, increasing food insecurity, and further straining Nigeria's finances as resources are redirected towards managing the conflict and hosting displaced persons.

https://doi.org/10.53477/2284-9378-25-16

**TABLE NO. 1**
**Insecurity Incidents vs. Federal Government Revenue and Revenue as % of GDP (2015-2024)**

| *Year* | Number of Insecurity Incidents | Federal Government Revenue (USD billion) | Government Revenue (% of GDP) |
|---|---|---|---|
| *2015* | 5,753 | 19.0 | 3.9% |
| *2016* | 6,349 | 16.2 | 4.0% |
| *2017* | 6,728 | 19.5 | 5.2% |
| *2018* | 7,003 | 22.0 | 5.2% |
| *2019* | 6,871 | 24.5 | 5.2% |
| *2020* | 7,985 | 14.3 | 3.3% |
| *2021* | 8,241 | 17.6 | 4.0% |
| *2022* | 9,121 | 20.8 | 4.4% |
| *2023* | 9,458 | 22.9 | 6.3% |
| *2024* | 9,700 | 24.1 | 6.6% |

**Sources:** Researcher's survey (2024) across various secondary materials; Nigeria GDP data from YCharts; Federal Government Revenue data from IMF Staff Country Reports.

The data illustrate a concerning trend where, despite a significant increase in insecurity incidents from 5,753 in 2015 to 9,700 in 2024, the federal government's revenue as a percentage of GDP has remained relatively low, fluctuating between 3.3% and 6.6% over the decade. This low revenue-to-GDP ratio suggests limited fiscal capacity to address the escalating security challenges and their associated socioeconomic impacts. The herder-farmer conflicts, particularly in states like Benue and Plateau, have not only led to loss of lives and displacement but have also strained the government's financial resources, diverting funds from developmental projects to security and humanitarian responses. This fiscal strain underscores the need for comprehensive strategies to enhance revenue generation and allocate resources effectively to mitigate the impacts of such conflicts.

### 3.5. Review of Empirical Studies

There have been various empirical studies on the effect of insecurity on public finance, and all of them show uniform findings emphasising raised defence expenditure, interrupted generation of revenue, and compromised allocation to social sectors. Eboh and Umahi (2021), in their research paper titled "Insecurity and Defence Spending in Nigeria: A Fiscal Challenge," analyse the fiscal impact of insecurity on Nigeria's budgetary process between 2008 and 2018. From their findings, based on secondary data collected from Nigeria's budgets and Central Bank of Nigeria (CBN) reports, it is evident that the issues of insecurity, like the Boko Haram menace, have led to the spending of over $16 billion on defence and more than 10% of the federal budget annually. By using trend analysis, they show how the rising number of terrorist attacks and banditry forced the Nigerian state to raise defence spending at the cost of the social sectors, such as health and education. Although trend analysis of defence spending is useful, their research has a limitation in examining how falling revenues due to insecurity constrain fiscal space in the long run, which remains an under-researched area.

Similarly, Olaniyan et al. (2022) also study how insecurity affects funding of the social sector in Nigeria. In "The Impact of Insecurity on Social Sector Funding in Nigeria," they analyse budgetary allocations to education and health amid rising defence spending. Employing comparative budgetary analysis during the 2010-2021 period, the authors conclude that, although defence funding continuously increased to over N500 billion in 2021, funding for education and health stagnated at less than 7% of the federal budget. This budget imbalance, they discover, has led to dismal social outcomes, particularly in northern Nigeria, where insecurity disrupts schooling and limits access to healthcare. The authors further indicate how insecurity has paralysed revenue generation in the war-torn areas, particularly in the agricultural sector, which provides a major percentage of Nigeria's non-oil revenue. Though the research aptly captures the trade-off between defence and social expenditure, it fails to capture the full macroeconomic dimension of the impacts, such as fiscal deficit, inflation, and exchange rate instability, which are equally exacerbated by insecurity.

More geographically focused is the study by Abdulkarim and Saidatulakmal (2022) on the fiscal impact of insecurity in northern Nigeria, 2015–2022. In "Fiscal Implications of Insecurity in Northern Nigeria: A Trend Analysis (2015–2022)," the authors present an assessment of the impact that insurgency, banditry, and farmer-herder conflicts have had on public finances in the area. Through the application of panel data methods and tracking key fiscal metrics, they establish that insecurity reduced agricultural output in northern Nigeria by 20%, resulting in reduced tax collections and economic stagnation. They further argue that the increased borrowing by the Nigerian government to fund defence and security operations worsened the debt crisis of the country with long-term impacts on fiscal sustainability. While providing useful data on inter-regional differentials in fiscal performances, their article lacks the inflationary pressures due to such fiscal imbalances and leaves scope for further study on the macroeconomic implications at a bigger level.

Comparative examination of war-torn different nations like Afghanistan and Somalia on an international scale provides useful lessons on the fiscal cost of insecurity. According to a 2018 International Monetary Fund report, prolonged insecurity in Afghanistan meant a shrinking tax base, increased defence expenditure, and over-reliance on foreign support to finance core government activities. Similarly, a 2020 World Bank review of Somalia presents the way insecurity disrupted agricultural production and trade, which led to fiscal imbalances, undermined governance, and limited the delivery of public services. These instances illustrate the long-term implications of putting defence spending ahead of social investment in countries ravaged by war. Although Nigeria's scenario is unique due to its relatively larger economy, the implication of these global examples is that defence spending needs to be complemented with investments in important social sectors for the purpose of fiscal sustainability.

In total, the studies under review all point to the ubiquity of the impact of insecurity on public finance, from higher defence expenditure to lower revenues and eroded

social investments. Yet, there is still much research to fill in gaps, notably concerning the macroeconomic effects of fiscal imbalances caused by insecurity. These include inflation, exchange rate volatility, and debt sustainability. Utilising the systems theory framework, this research seeks to fill these gaps by investigating the ways in which insecurity, as a structural factor, destabilises fiscal stability and affects other sectors within Nigeria's public finance system. Through this method, the study will yield a better comprehension of the nexus between insecurity and fiscal sustainability and, in the process, enrich the larger academic literature on conflict, governance, and public finance in fragile states.

## 4. Results Presentation and Data Analysis

### *4.1. Comparative analysis of Nigeria's fiscal expenditures across 5 Sectors*

**TABLE NO. 2**
**Nigeria Federal Budget Allocations and Economic Indicators (2015-2024) in Naira**

| Year | Education (₦ Trillion) | Health (₦ Trillion) | Agriculture (₦ Trillion) | Defence (₦ Trillion) | Debt Servicing (₦ Trillion) | Inflation Rate (%) |
|---|---|---|---|---|---|---|
| 2015 | 0.484 | 0.296 | 0.040 | 0.414 | 1.0 | 9.0 |
| 2016 | 0.403 | 0.250 | 0.046 | 0.516 | 1.23 | 15.7 |
| 2017 | 0.550 | 0.308 | 0.051 | 0.495 | 1.8 | 16.5 |
| 2018 | 0.605 | 0.356 | 0.118 | 0.612 | 2.01 | 12.1 |
| 2019 | 0.620 | 0.424 | 0.083 | 0.676 | 2.40 | 11.4 |
| 2020 | 0.686 | 0.427 | 0.183 | 0.943 | 2.40 | 13.2 |
| 2021 | 0.771 | 0.547 | 0.179 | 1.341 | 3.00 | 16.5 |
| 2022 | 0.923 | 0.876 | 0.284 | 1.579 | 3.76 | 18.6 |
| 2023 | 1.079 | 1.097 | 0.228 | 3.250 | 7.66 | 21.0 |
| 2024 | 2.180 | 1.330 | 0.228 | 4.910 | 8.10 | 19.5 |

**Sources:** Data compilation from NBS, Statista.

**TABLE NO. 3**
**Nigerian Federal Budget Allocations (USD) Across Key Sectors (2015–2024)**

| Year | Education (USD Billion) | Health (USD Billion) | Agriculture (USD Billion) | Defence (USD Billion) | Debt Servicing (USD Billion) | Inflation Rate (%) |
|---|---|---|---|---|---|---|
| 2015 | 2.46 | 1.50 | 0.20 | 1.95 | 3.50 | 9.01 |
| 2016 | 1.32 | 0.82 | 0.15 | 2.00 | 4.37 | 15.68 |
| 2017 | 1.53 | 0.86 | 0.14 | 2.19 | 5.03 | 16.52 |
| 2018 | 1.67 | 0.98 | 0.33 | 2.28 | 5.60 | 12.10 |
| 2019 | 1.72 | 1.18 | 0.23 | 2.35 | 5.67 | 11.40 |
| 2020 | 1.81 | 1.12 | 0.48 | 2.91 | 6.36 | 13.25 |
| 2021 | 1.88 | 1.33 | 0.44 | 3.35 | 7.70 | 16.98 |
| 2022 | 2.15 | 2.04 | 0.66 | 4.02 | 9.02 | 18.81 |
| 2023 | 1.40 | 1.42 | 0.30 | 4.35 | 9.45 | 21.80 |
| 2024 | 2.76 | 1.68 | 0.29 | 4.80 | 10.35 | 22.50 |

**Sources:** Researchers' compilation from NBS, CBN, Statista across various years.

*The table provides a decade-long (2015–2024) overview of Nigeria's budget allocations to key sectors such as education, health, agriculture, defence, and debt servicing, alongside annual inflation rates. Over this period, defence spending witnessed a consistent increase, reflecting Nigeria's heightened security challenges, especially due to insurgency, banditry, and herder-farmer conflicts. Defence spending surged from $1.95 billion in 2015 to $4.80 billion in 2024, underscoring how insecurity has dominated fiscal priorities. Conversely, allocations to education, health, and agriculture remained relatively stagnant or saw minor fluctuations, with education experiencing a drop to $1.32 billion in 2016 before increasing modestly, and agriculture receiving consistently low funding, peaking at $0.66 billion in 2022. On the other hand, debt servicing rose significantly, from $3.50 billion in 2015 to $10.35 billion in 2024, reflecting Nigeria's mounting debt burden due to fiscal deficits and external borrowings. Meanwhile, inflation rates also climbed, particularly after 2020, from 13.25% to 22.50% by 2024, driven by the economic impact of insecurity, devaluation of the naira, and global shocks such as COVID-19. The data highlights how rising debt servicing and defence spending constrained funding for critical social services, which may have worsened human capital development outcomes and agricultural productivity.*

https://doi.org/10.53477/2284-9378-25-16

***Government Expenditure across military outfits (2015-2025)***

**TABLE NO. 4**
**Nigerian Government Expenditure on Security per Force (2015-2025)**

| Year | Army (Naira) | % Growth | Navy (Naira) | % Growth | Air Force (Naira) | % Growth |
|---|---|---|---|---|---|---|
| 2015 | ₦150 billion | - | ₦75 billion | - | ₦77 billion | - |
| 2016 | ₦148 billion | -1.33% | ₦86 billion | +14.67% | ₦91 billion | +18.18% |
| 2017 | ₦155 billion | +4.73% | ₦90 billion | +4.65% | ₦100 billion | +9.89% |
| 2018 | ₦224 billion | +44.52% | ₦97 billion | +7.78% | ₦112 billion | +12% |
| 2019 | ₦228 billion | +1.79% | ₦101 billion | +4.12% | ₦115 billion | +2.68% |
| 2020 | ₦463 billion | +103.07% | ₦131 billion | +29.70% | ₦136 billion | +18.26% |
| 2021 | ₦511 billion | +10.38% | ₦136 billion | +3.82% | ₦140 billion | +2.94% |
| 2022 | ₦579 billion | +13.31% | ₦148 billion | +8.82% | ₦180 billion | +28.57% |
| 2023 | ₦580 billion | +0.17% | ₦113 billion | -23.65% | ₦184.77 billion | +2.65% |
| 2025 | ₦19.2 billion* | -96.69%* | ₦514.4 million* | -99.55%* | ₦39.5 billion* | -78.62%* |

**Sources:** Researchers' compilation, 2025

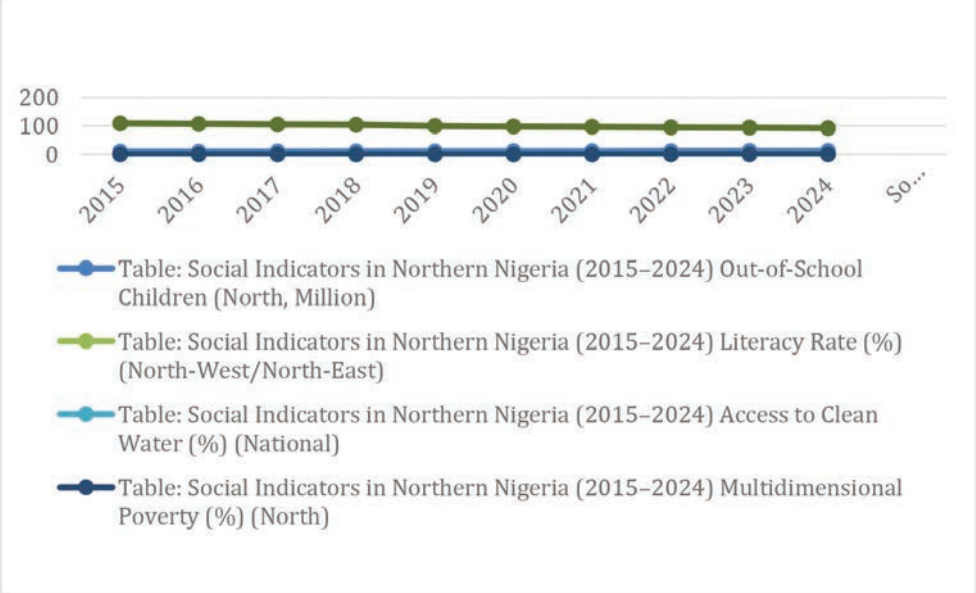
*The table presents Nigerian government expenditure on the Army, Navy, and Air Force from 2015 to 2025, along with the percentage growth in allocations for each year. Between 2015 and 2022, there is a general upward trend in defence spending, with the Army seeing the largest increase, particularly from 2020 onward, when allocations rose dramatically, reaching 579 billion in 2022. This spike corresponds with escalating insecurity across the country, including Boko Haram insurgency, banditry, and herder-farmer conflicts. Similarly, allocations to the Navy and Air Force also increased, though at varying rates, with notable jumps in 2020 due to increased security pressures.*

**TABLE NO. 5**
**Social Indicators in Northern Nigeria (2015-2024)**

| Year | Out-of-School Children (North, Million) | Literacy Rate (%) (North-West/North-East) | Access to Clean Water (%) (National) | Multidimensional Poverty (%) (North) | Child Mortality (per 1,000 births) |
|---|---|---|---|---|---|
| 2015 | 10.5 | 49% / 40% | 29% | 70% | 109 |
| 2016 | 10.9 | 50% / 42% | 30% | 71% | 107 |
| 2017 | 11.3 | 51% / 43% | 32% | 73% | 105 |
| 2018 | 11.5 | 53% / 45% | 35% | 74% | 104 |
| 2019 | 11.8 | 54% / 46% | 37% | 75% | 100 |
| 2020 | 12.0 | 55% / 47% | 40% | 76% | 98 |
| 2021 | 12.3 | 57% / 48% | 42% | 78% | 97 |
| 2022 | 12.5 | 59% / 49% | 45% | 78% | 95 |
| 2023 | 13.0 | 60% / 50% | 46% | 79% | 94 |
| 2024 | 13.2 | 62% / 51% | 47% | 80% | 92 |

**Sources:** Researchers' compilation across various organisations

**Graphical representation of social indicators in Northern Nigeria**




***Discussion of Findings: Public Expenditure Trends in Nigeria (2015-2024)***

The budgetary allocation trends in Nigeria between 2015 and 2024 indicate a troubling fiscal imbalance, driven largely by the country's deteriorating security situation. While core social sectors like education, health, and agriculture budgets show incremental increases over the years, the disproportionate rise in security spending reflects Nigeria's struggle with protracted insecurity, particularly in Northern Nigeria, where insurgency, banditry, and farmer-herder conflicts have disrupted socio-economic activities. The surge in security expenditures during this period is symptomatic of Nigeria's reactive fiscal approach to insecurity. Scholars like Collier (2007) argue that excessive military expenditure in fragile states often reduces the fiscal space needed for investment in human capital and social infrastructure. This trade-off is evident in

Nigeria's budget allocations, whereby while military spending rose from ₦302 billion in 2015 to over ₦1.04 trillion in 2022, education, health, and agriculture allocations remained comparatively stagnant, failing to meet international benchmarks. For example, UNESCO recommends that nations allocate 15–20% of their national budgets to education. However, Nigeria's education budget consistently falls short of this target, peaking at just 7.9% in 2024. Similarly, the World Health Organization (WHO) advises that at least 5% of a country's GDP should be allocated to health, but Nigeria's health budget, although increasing, remains insufficient to meet the population's needs, particularly in conflict-affected areas where hospitals have been destroyed, and healthcare delivery is severely disrupted.

The fiscal structure of a country plays a vital role in shaping social development outcomes, as seen when comparing Norway and Nigeria. Norway's well-structured fiscal policies emphasise effective management of oil revenues, with substantial allocations toward education, healthcare, and social welfare. This strategic focus has contributed to Norway achieving some of the best global social indicators, including an under-5 mortality rate of just 2 per 1,000 live births and a Human Development Index (HDI) score of 0.965, ranking it among the highest globally. Conversely, Nigeria's fiscal framework has struggled to effectively address social challenges, particularly due to competing priorities such as defence spending. In 2015, Nigeria recorded an under-5 mortality rate of 109 per 1,000 live births, which, while declining to 88 per 1,000 by 2024, still lags behind many middle-income countries. Additionally, Nigeria's HDI score stagnated at around 0.539 by 2020, reflecting limited progress in human capital development. This comparison highlights how a nation's fiscal policy and prioritisation can either drive or hinder social progress, with investments in critical sectors directly influencing key human development metrics (UNICEF 2020).

*Table showing data for Nigeria from 2015 to 2024 on child mortality rates, standard of living indicators, and multidimensional poverty indices:*

| Year | Under-5 Mortality Rate (per 1,000 live births) | Human Development Index (HDI) | Multidimensional Poverty Index (MPI) |
|---|---|---|---|
| 2015 | 109.0 | 0.527 | 0.3 |
| 2016 | 106.0 | 0.528 | 0.27 |
| 2017 | 104.0 | 0.531 | 0.257 |
| 2018 | 100.0 | 0.534 | Data not available |
| 2019 | 98.0 | 0.538 | Data not available |
| 2020 | 96.0 | 0.539 | 0.11 |
| 2021 | 94.0 | 0.535 | 0.3 |
| 2022 | 92.0 | 0.534 | 0.25 |
| 2023 | 90.0 | Data not available | 0.17 |
| 2024 | 88.0 | Data not available | 0.257 |

**Sources:** Researchers' compilation from various organisations

The data findings reveal the broader social challenges linked to Nigeria's fiscal shift toward military and defence spending from 2015 to 2024. Nigeria's case is mirrored by Iraq, another resource-rich nation whose fiscal reallocation toward defence has hindered social development. In Iraq, heavy defence expenditures following years of insurgency have constrained investments in critical social sectors. Despite Iraq's oil wealth, the country recorded an under-5 mortality rate of 25 per 1,000 live births in 2020, far higher than neighbouring oil-exporting countries like Saudi Arabia, where the rate is 6 per 1,000. Similarly, Iraq's Human Development Index (HDI) stagnated at 0.674 in 2020, while Saudi Arabia's stood at 0.854, reflecting Iraq's struggle to balance defence priorities with broader human capital investments. Nigeria faces parallel issues. Despite a decline in its under-5 mortality rate from 109 per 1,000 in 2015 to 88 in 2024, the slow progress underscores insufficient investment in healthcare due to fiscal diversion.

The agricultural sector has also suffered from both insecurity and inadequate funding. Armed violence, particularly in Northern Nigeria, has displaced thousands of farmers, reduced access to farmlands, and disrupted food supply chains. This has exacerbated food insecurity, with the Global Hunger Index ranking Nigeria 103rd out of 121 countries in 2022, citing insecurity as a key driver of declining agricultural productivity. Yet, despite these challenges, agricultural funding has remained erratic, peaking at 0.284 trillion in 2022 but dropping to 0.228 trillion in 2024. This disconnection between the scale of the agricultural crisis and government funding allocations reflects what Amartya Sen (1981) describes as a failure to prioritise social protection in times of crisis. Without adequate investment in agricultural resilience, Nigeria risks deepening rural poverty and food insecurity, further fuelling the cycle of violence in agrarian communities.

This situation Nigeria finds itself in, with shifting budgetary priorities, can be linked to key security events that have shaped the country's fiscal landscape. For instance, the escalation of Boko Haram attacks in the Northeast following the 2014 Chibok schoolgirls' abduction led to a sharp increase in defence spending in subsequent years. Similarly, the rise in banditry and kidnappings in the Northwest between 2018 and 2021 prompted increased allocations for military operations like Operation Hadarin Daji and Operation Sharan Daji. Despite these increased expenditures, the efficacy of Nigeria's military response remains questionable. Reports from the International Crisis Group (2021) highlight the fact that, while security forces have achieved some tactical but temporary victories, the underlying drivers of insecurity, such as poverty, unemployment, and weak governance, remain largely abates due to the underfunding of social sectors which are supposed to strengthen peace.

Insecurity cuts across various sectors; some of them are education, agriculture and health, which have gotten less traction from the government. Development needs peace and peace needs development, making them sine qua non to each other (UNDP 2021). However, Nigeria has tried to fight insecurity by enforcing peace

without tackling the cogent instigator of insecurity in the Northeast, which is characterised by underdevelopment and low human capital development. The disproportionate allocation of resources to security creates a vicious cycle, wherein inadequate investment in education, health, and agriculture exacerbates the very conditions that fuel insecurity. Nigeria's youth unemployment rate, for instance, was at over 40% in 2023, with limited job opportunities contributing to the recruitment of young people by armed groups. The health sector faces similar challenges. The disruption of healthcare services in conflict zones has led to rising maternal and child mortality rates, while the underfunding of healthcare infrastructure in safer regions limits Nigeria's capacity to address public health crises. This situation has prompted calls from policymakers and civil society organisations for a more balanced approach to national security, one that emphasises human security as much as territorial security. If current trends continue, Nigeria risks further entrenching its fiscal imbalance, with security spending crowding out critical investments in social sectors. This could have long-term implications for the country's development trajectory. As the United Nations Development Programme (UNDP) warns, countries that prioritise military spending at the expense of education, health, and social protection often experience slower economic growth, higher inequality, and prolonged instability. However, there are opportunities for Nigeria to reverse this trend by fighting insecurity on all sectors.

**5. Summary of Findings**

The data indicate that Nigeria's response to insecurity of lives and property has necessitated significant defence spending, which has, in turn, constrained investments in essential social services. However, this reallocation poses risks to long-term development, as underfunded education and health sectors have led to a less educated and less healthy workforce, perpetuating cycles of poverty and instability. The increase in multi-dimensional poverty across the country, with an increased child mortality rate, internally displaced population, and reduced standard of living and propensity to live, showcases the adverse effect of the protracted insecurity in the North and the reallocation of funds effect. Comparatively, the experience of other nations facing protracted conflicts suggests that without a balanced approach that addresses both security and social needs, achieving sustainable peace and development remains challenging.

## Conclusion

The frailty of Nigeria's polity and economy is based on cumulative factors and stressors that have either been swept under the rug or partially rectified, which in the fourth republic now creates a sporadic and colossal effect on all other sectors. This is what has caused, over the last decade, Nigeria to continue its reactive dance to the tune of insecurity in Northern Nigeria, which has profoundly impacted public finance, compelling the government to allocate substantial resources to defence at

the expense of social sectors. This problem indicates the fragile nature of Nigerian political and socioeconomic conditions, which makes events affect the overall national economy.

**Recommendations**

The structural issue of Nigeria's porous borders has been superficially addressed by successive governments. For over 60 years, Nigeria has lacked a concrete and sustainable plan for border demarcation and security. Despite the serious threats posed by porous borders, they have not received the level of security attention they urgently require. This research recommends that addressing Nigeria's insecurity must begin with a comprehensive review and the adoption of an integrated approach to border management and security. Therefore, a specialised institutional framework should be developed under military oversight, designed specifically for border control, similar to the U.S. Border Patrol. This body would function as an independent and well-structured border force, distinct from the existing Customs and Immigration Services, which are primarily focused on revenue generation and minimal border enforcement. By establishing a dedicated and well-equipped border protection unit, Nigeria can enhance border security and reduce the infiltration of criminal elements, thus contributing significantly to addressing the country's broader insecurity challenges.

## References

**Abdulkarim, M., and M. Saidatulakmal.** 2022. "Growth and Fiscal Effects of Insecurity on the Nigerian Economy." *Journal of Economic Studies* 49 (3): 456–472.

**African Development Bank.** 2022. *African economic outlook 2021: From debt resolution to growth—The road ahead for Africa.* Abidjan: AfDB. https://www.afdb.org/en/documents/african-economic-outlook-2021.

**African Union Peace and Security Council.** 2015. *Report of the Chairperson of the Commission on regional and international efforts to combat the Boko Haram terrorist group and the way forward.* Addis Ababa: African Union. https://www.peaceau.org.

**Aganga, O.** 2023. *Reclaiming the Jewel of Africa: A Blueprint for Taking Nigeria and Africa from Potential to Posterity.* Practical Inspiration Publishing.

**Ake, C.** 1996. *Democracy and development in Africa.* Washington, D.C.: Brookings Institution.

**Armed Conflict Location & Event Data Project [ACLED].** 2024. *Nigeria: Conflict data overview 2015–2024.* Retrieved from https://acleddata.com.

**Budget Office of the Federation.** 2022. *Federal government of Nigeria approved budget 2022.* Abuja: Budget Office. Retrieved from https://www.budgetoffice.gov.ng.

**Central Bank of Nigeria [CBN].** 2017. "Annual statistical bulletin 2016." Abuja. Retrieved from https://www.cbn.gov.ng.

**___.** 2023. "Annual Statistical Bulletin 2023: Government Finance and Economic Trends." Retrieved from https://www.cbn.gov.ng.

**Collier, P.** 2007. *The bottom billion: Why the poorest countries are failing and what can be done about it.* Oxford University Press.

**Collier, P., and A. Hoeffler.** 2004. "Greed and grievance in civil war." *Oxford Economic Papers* 56 (4): 563–595. https://doi.org/10.1093/oep/gpf064.

**Council on Foreign Relations.** 2023. *Nigeria Security Tracker (NST): Trends in Insecurity and Violence.* https://www.cfr.org/nigeria-security-tracker.

**Easton, D.** 1971. *The Political System: An Inquiry into the State of Political Science.* (2nd ed.). Knopf.

**Eboh, C., and D. Umahi.** 2021. "Insecurity and Defense Spending in Nigeria: A Fiscal Challenge."

**Federal Ministry of Finance, Budget, and National Planning.** 2024. *Annual Budget Performance Reports.* Retrieved from https://budgetoffice.gov.ng.

**Federal Republic of Nigeria.** 2015. "National Counter Terrorism Strategy (NACTEST). Office of the National Security Adviser." Retrieved from https://ctc.gov.ng.

**Global Terrorism Index.** 2022. *Measuring the impact of terrorism 2022.* Sydney: Institute for Economics & Peace. https://www.visionofhumanity.org/maps/global-terrorism-index/.

**Institute for Economics & Peace [IEP].** 2022. *Global terrorism index 2022: Measuring the impact of terrorism.* https://www.economicsandpeace.org/wp-content/uploads/2022/03/GTI-2022-web.pdf.

**International Crisis Group [ICG].** 2021. *Violence and Insecurity in Nigeria's Northern Region: Analyzing Root Causes.* Brussels: International Crisis Group.

**International Monetary Fund [IMF].** 2018. "Islamic Republic of Afghanistan: Staff Report for the 2018. Article IV Consultation and Request for a Three-Year Arrangement Under the Extended Credit Facility." IMF Country Report No. 18/127. https://www.imf.org/-/media/Files/Publications/CR/2018/cr18127.ashx.

**___.** 2023. *Fiscal Monitor: Navigating Global Shocks and Uncertainty.* Washington, DC: International Monetary Fund.

**Multinational Joint Task Force [MNJTF].** 2021. *MNJTF sustains counterinsurgency efforts in Lake Chad Basin region.* https://mnjtffmm.org.

**Musgrave, R.A., and P.B. Musgrave.** 1989. *Public finance in theory and practice.* (5th ed.). New York: McGraw-Hill.

**National Bureau of Statistics [NBS].** 2023. *Nigeria Poverty and Inequality Report: Socioeconomic Impact of Insecurity.* Abuja: NBS. Retrieved from https://www.nigerianstat.gov.ng.

**Nigeria Budget Office of the Federation.** 2024. "Annual Budget Reports (2015–2024)." Retrieved from https://budgetoffice.gov.ng.

**Nigeria Economic Summit Group [NESG].** 2023. *Fiscal Constraints and National Development: Security Challenges and Implications for Public Finance.* Lagos: NESG Publications.

**Nigerian Army.** 2015. *Operation Lafiya Dole launched to intensify fight against Boko Haram.* Nigeria: Ministry of Defence. Retrieved from https://army.mil.ng.

**Nigeria Security Tracker [NTS].** 2023. *Insecurity Trends in Nigeria: Violence and its Fiscal Impacts.* Washington, DC: Council on Foreign Relations.

**Olaniyan, T., J. Adekunle, and F. Osagie.** 2022. *The Impact of Insecurity on Social Sector Funding in Nigeria.*

**Oxford Business Group.** 2024. *Nigeria economy report 2024: Fiscal restructuring and revenue diversification.* https://oxfordbusinessgroup.com/reports/nigeria.

**Rezai, A., F. Ruch, R. Choudhary, and J.N.D. Francois.** 2024. "Fiscal policy's role in economic resilience to climate shocks ." Policy Research Working Paper No. 10982, World Bank. https://hdl.handle.net/10986/42456.

**Statista.** 2024. *Defense expenditure in Nigeria from 2015 to 2024.* https://www.statista.com/statistics/1343802/nigeria-defense-budget/.

**Stockholm International Peace Research Institute [SIPRI].** 2023. "Trends in world military expenditure, 2022." SIPRI Fact Sheet. https://www.sipri.org/publications/2023/sipri-fact-sheets/trends-world-military-expenditure-2022.

**United Nations Development Programme [UNDP].** 2021. *The Human Cost of Insecurity in Nigeria.* New York: UNDP Publications.

**UNHCR.** 2022. *Nigeria emergency. United Nations High Commissioner for Refugees.* Retrieved from https://www.unhcr.org/ng.

**UNICEF.** 2020. *Progress for Every Child in the SDG Era: Statistical Update.* United Nations Children's Fund.

**World Health Organization [WHO].** 2022. *Health in Conflict Zones: The Impact of Armed Violence on Access to Health Services in Nigeria.* Retrieved from https://www.who.int.

**Wolfers, A.** 1952. ""National security" as an ambiguous symbol." *Political Science Quarterly* 67 (4): 481–502. https://doi.org/10.2307/2145138.

**World Bank.** 2020. *Somalia Economic Update: Impact of COVID-19—Policies to Manage the Crisis and Strengthen Economic Recovery.* https://documents1.worldbank.org/curated/en/252881595627954924/pdf/Somalia-Economic-Update-Impact-of-COVID-19-Policies-to-Manage-the-Crisis-and-Strengthen-Economic-Recovery.pdf.

**___.** 2023. *Nigeria Economic Update: Resilience through Reforms* . Washington, DC: World Bank Publications.

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

# Provision of Food for the Population of Polish Urban Agglomerations during the War of 1939. Plans and their Implementation on the Example of Warsaw

**Grzegorz JASIŃSKI, PhD***
*Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego
e-mail: grzegorz.jasinski@wat.edu.pl

## Abstract

The subject of battlefield logistics security in some countries lies outside the mainstream of military historians' studies of armed conflicts in the broadest sense. This is surprising insofar as these activities almost always determine the manner and possibilities of conducting military operations. For example, this issue can be seen in the Polish literature on the defensive war of 1939. Although several comprehensive studies have been written, significant gaps remain in many areas, hindering a proper understanding of various aspects of the September 1939 fighting. One such topic is the preparation of the Polish civilian and military administration to meet the food needs of the civilian population in urban agglomerations in September 1939. The purpose of this article is to show the inadequacies of Polish preparations against the background of German efforts in this regard and to determine what effect victualling had on the ability to conduct a prolonged and organized defense. For this purpose, the author will use the example of one of the longest-defending urban centers in September 1939, namely the Polish capital, Warsaw.

**Keywords:**
Food provisions, 1939 defensive war, defense of Warsaw, Polish Army.

**Article info**
Received: 12 May 2025; Revised: 5 June 2025; Accepted: 10 June 2025; Available online: 27 June 2025

Citation: Jasiński, G. 2025. "Provision of Food for the Population of Polish Urban Agglomerations during the War of 1939. Plans and their Implementation on the Example of Warsaw" *Bulletin of "Carol I" National Defence University*, 14(2): 82-92. https://doi.org/10.53477/2284-9378-25-17

## Organization of feeding the population of cities in the German Reich under conditions of armed conflict. Legal regulations and organizational preparations

After the end of World War I, many European countries recognized the need to develop an organized and more efficient victualling system for emergencies and war. This task took on particular importance in the German Reich after Hitler came to power. As early as September 13, 1933, a law was passed regulating the area of victualling (*Gesetz über denvorläufigen Aufbau des Reichsnährstandes und Maßnahmen zur Markt- und Preisregelung für landwirtschaftliche Erzeugnisse*), the so-called „Reichsnahrstandsgesetz", under which Walther Darré Minister of Food and Agriculture of the Reich (*Reichsminister für Ernährung und Landwirtschaft*) was given broad powers to regulate, produce and market agricultural commodities (Rodziewicz 2022, 223). Among other things, tens of thousands of local organizations of agricultural producers and processors, and more than a dozen union headquarters were merged. The following year also saw the start of construction of a state network of elevators with a capacity of 5,000 to 70,000 tons. As a result, the Reich Food Farm (*Der Reichsnährstand*) had 8.8 million tons of grain stockpiled in 1939, which could have supplied the German non-farming population with bread for more than a year (Münkel 1996, 485). At the same time, imports of animal and vegetable products were launched on a large scale, which, as early as 1935, made it possible to reduce social tensions and provide a far higher level of provisioning for the first months of the war than before. Thanks to good harvests in 1938 and 1939, supplies were also plentiful. A level of self-sufficiency in grain, potatoes, sugar, and meat was achieved. A few weeks before the outbreak of war, Germany reached a self-sufficiency rate of 83 percent, a significant increase from the 68 percent in 1928 (Volkmann 2003, 372).

In 1937, work began on developing a universal victualling system for urban agglomerations (Łuczak 1982, 282). An elaborate system of collection and distribution of foodstuffs was created, which employed 2.5 million people (Rodziewicz 2022, 235). Since the main industrial centers and state institutions were concentrated in the cities, their employees were to be assured of receiving daily food at feeding stations organized there. Pre-school and school children, on the other hand, were to receive meals at the institutions they attended. Non-working persons were to receive meals at community kitchens specially established for this purpose. The standard due included one hot meal and appropriate food allotments for breakfast and dinner. In addition, a special category of people was singled out who, among other reasons, the need to move, could not be covered by the general victualling system, and for them, food cards were designated, allowing them to purchase basic foodstuffs and prepare their own meals. The food ration cards were to be delivered by specially designated persons who were not subject to conscription (Urliński 2009, 133).

In 1938, planning work had already begun to take on a very tangible character. During the summer, work was carried out in industrial plants under the slogan

"warm food for workers," in the course of which appropriately grouped victualling units responsible for providing food for workers were formed from plants and enterprises. Also, starting in September, the gradual implementation of collective feeding in cities for workers began (Urliński 2009, 133). Beginning in 1939, large-scale propaganda efforts were launched to familiarize the civilian population with the need to introduce collective feeding and uniform meals. Mandatory rationing, however, was not introduced after the war began. From September 1, 1939, only fat, meat, butter, milk, cheese, sugar, and jam were available on ration cards, and from September 25, additionally bread and eggs. Despite these restrictions, food rations for the civilian population were relatively high at the time, around 2,600 kcal (Volkmann 2003, 393).

It should be noted that in view of the tense food situation in the Reich, at the beginning of the aggression against Poland it was ordered in the quartermaster's directives in the army, that in the occupied enemy territory, as far as possible, full supplies for men and horses should be taken from the area. This meant basing supplies on looting conquered territory (National Archives 1939).

## Plans for supplying the population of Polish cities with food in case of war and their implementation on the example of Warsaw

After Poland regained its independence in 1918, the following years brought struggles to shape the post-war borders and maintain sovereignty. While they were still going on, the economic reconstruction of the lands, extremely damaged as a result of World War I, began, as well as their unification due to more than a century of partition history. The scale of the challenges facing the authorities of this emerging state from non-being was enormous. In addition, the geopolitical situation already in place after the formation of the borders necessitated the maintenance of a large military. The Versailles order was not sustainable, and the threat from both the West and the East was real. The deterioration of the international situation in the second half of the 1930s led to an even more radical re-evaluation in the policy of the authorities of the time and an increase in military capabilities, and consequently, the importance of economic matters oriented in terms of state defense increased. As a result, in 1936, the Committee for the Defense of the Republic (KOR) was established, which, through its secretariat - SeKOR, headed by Brig. Gen. Tadeusz Malinowski, was to coordinate the preparation of the state's war-economic potential in the event of an impending armed conflict. However, in March 1936, in a study entitled "Provisioning for War", a group of military specialists warned the public opinion that no coordinated work had been carried out so far on providing provisions for the population and armed forces in time of war, and that it was urgent to begin developing appropriate plans (Urliński 2009, 115).

In interwar Poland, free trade was the primary form of procurement of needed materials and food. However, this system could not work under wartime conditions, so for emergencies, including war, it was decided to introduce rationed supplies for selected products supplemented by free market sales. Obtaining the necessary mass of products to cover the needs of the rationed market and the army required the introduction of benefits in kind. On the basis of statutory regulations in this regard, plans were drawn up in the second half of the 1930s: the victualling of the armed forces „Apr. IV" and the victualling of the civilian population „Apr. IX".

According to the first, the quartermaster authorities of the Polish Army were to accumulate food supplies in depots and warehouses for 8 days of fighting, which together with the supply of soldiers' starting equipment (5 days together with 2 days of "R" rations) was to be sufficient for a total of 15 days of warfare. After this period, the victualing of the combatants should be fully ensured by the civilian authorities, although it is worth noting that from the tenth day after the announcement of mobilization, the army could use the supplies accumulated in warehouses filled by the civil administration (Sulisławski 1939, 5). This system, however, was not adapted to the maneuvering nature of operations in the coming conflict and, due to the rapid loss of areas that served as supply bases and the dramatic outright shortage of wheeled and rail transportation, further paralyzed by aviation operations, it did not work well in the 1939 defensive war. Nevertheless, the development of plans for the provisioning of the civilian population and their implementation presented a much worse picture.

Poland was an agricultural country, and for this reason, in terms of provisioning, the rural population was considered fully self-sufficient. The population of small cities and towns was treated similarly. Only large urban agglomerations were to be covered by the victualling plans. Supply rationing and normalization of consumption according to previously developed standards and recommendations were to be introduced. To this end, in February 1938, an Undersecretariat of State was created in the Ministry of Agriculture and Agrarian Reform (MARD) to deal with all the country's victualling matters, and the creation of victualling offices in large agglomerations began (Prezydenta Rzeczypospolitej 1938). The Ministry of Internal Affairs, realizing the delays in this regard, intended to develop an ad hoc plan very quickly, followed by the aforementioned "Apr. IX" basic plan.

In late June/early July 1938, Deputy Minister in the Ministry of Internal Affairs Michal Wierusz-Kowalski sent a document with the title "Guidelines for Developing Materials for Provisioning Cities" to all provincial governors for distribution to city mayors. In it, a general planning concept was defined, and the need to assess the needs, the possibility of covering them, and the distribution of food by existing provisioning cells was expressed. To this end, eight groups of issues were identified around which work was to be conducted:

1. population of the city;
2. current size of annual consumption of each product;

3. share of each mode of transport in deliveries to the city of a particular product;
4. general conditions characterizing the supply capacity of the city;
5. characteristics of the collection and distribution apparatus;
6. characteristics of technical equipment;
7. processing;
8. characteristics of stocks held in warehouses (Dokumenty Sekretariatu Obrony Rzeczpospolitej 1938, Ref. I.303.13.74).

In order to determine in detail which cities and industrial and suburban centers are to be included in the victualling plan and which cities are to be supplied outside the victualling plan, a preliminary classification of all cities and industrial and suburban centers was made in the Ministry of the Interior. It was initially assumed that cities with a population of more than 50,000 might run out of food under wartime conditions, and there would be a need for local governments to support subsistence needs. However, finally in the summer of 1938, a division of urban agglomerations into three groups was adopted: Group I included those cities with a population of more than 100,000, which were to have victualing offices (branches) established, pursuant to a circular of the Ministry of Internal Affairs dated March 28, 1938. Group II included those cities with a population of less than 100,000, which were important industrial, commercial, administrative, etc., centers, and were located in agricultural districts with insufficient productivity to supply these cities. The basic form of supplying rationed materials in both of these groups of cities was to be the card system. In contrast, cities outside Groups I and II constituted Group III. Supplying these cities was to be done outside of the victualling plan being developed (Dokumenty Sekretariatu Obrony Rzeczpospolitej 1939, Ref. I.303.13.74).

According to surviving documents, it appears that materials at the level of city boards were to be prepared by October 1938. However, on September 9th, further "Guidelines for developing the degree of victualling security of the city" were published. (Urlinski 123 and 124). They ordered city boards, among other things, to take into account that under wartime conditions it would not be possible to transport food products by rail, and that wheeled deliveries of certain products would be reduced by half. For this reason, municipal victualling authorities were to dispose of supplies in previously prepared warehouses and depots. They also specified the norm of daily consumption per capita: rye flour 225 g, wheat flour - 50 g, meat 100 g, edible fats 40 g, potatoes - 500 g, legumes - 50 g, groats 50 g, sugar 25 g, eggs - 0.5 pieces, milk 0.1 l, coal - 5 kg, firewood 0.15 kg, soap 5 g (Dokumenty Sekretariatu Obrony Rzeczpospolitej 1938, Ref. I.303.13.74).

The compilation of basic data at the level of municipal boards was very slow. For this reason, by a decision of the Ministry of Military Affairs on April 26th, 1939, professional cadres were sent to government and local administration offices to serve as victualling inspectors (Dokumenty Sekretariatu Obrony Rzeczpospolitej 1939,

Ref. I.303.13.74). However, due to the shortage of specialized intendant officers, this decision was carried out only in part and did not significantly affect the work on victualling preparations underway in urban centers. The poor state of preparations in this regard was even reported in the press in the summer of 1939. As a result of this, as well as growing Polish-German tensions, on July 27th, the Ministry of the Interior drafted further guidelines, "Provisional Guidelines for the Preparation and Operation of the City Supply Plan," and on August 7th, 1939. "Guidelines for Governors on the Preparation and Launch of the City Supply Plan" (Urliński 2009, 126). According to them, victualling food products covered by the state-wide plan were subject to standardization. Products in free or controlled circulation were to reach the civilian population through municipal victualling bodies, as a result of stockpiling or commercial activities. The plan was not to be fully activated until the fifth week after mobilization was announced. The guidelines also included an organizational chart of the victualling bodies for cities in Groups I and II. At the head was the mayor of the city, who, upon the announcement of general mobilization or the outbreak of war, established a Provisioning Department or Branch. This was an administrative body responsible for the basic elements related to the functioning of the city's victualling apparatus. The mayor also established the City Provisioning Department, which included cooperative and private establishments. It was responsible for carrying out the tasks provided for in the state-wide plan, as well as in the local plan. In addition, a separate group of tasks was envisaged to be carried out by representatives of the urban community, organized into the Provisioning Committee, which was to serve as a liaison between the population and representatives of the municipal provisioning apparatus (Urliński 2009, 129-132).
Despite numerous initiatives and months of formal and legal preparations, most organizational activities, including stockpiling, were implemented in urban centers only in the summer of 1939, in addition, in a manner that was not coordinated with the plans, tasks, and needs of the Polish Army.

At the outbreak of World War II, Warsaw was the only city in Poland with a population of more than 1 million (about 1 million 300,000). The Vistula, one of the country's two largest rivers, flowing through it, divides it in half. The capital, located in the center of the country, was a major political and administrative center, as well as the most important railroad hub. Originally, there were no plans to defend it. For this reason, the main tasks of the District Corps Command No. I (DOK I) for the duration of the conflict were primarily to carry out mobilization activities and to supply war material and food to the two, and in time, even four all-military armies fighting in the west of the country, several hundred kilometers away from the city. In accordance with the nationwide victualling plan, during the first two weeks of hostilities, the quartermaster's office of DOK I was to organize ongoing supplies of meat and soldiers' bread to the front. The daily demand for bread alone for the two armies thus amounted to 330,000 to 350,000 loaves, which had to be baked, transported to railroad stations, transported to the supply area, and then properly distributed, and all this under combat conditions (Jasiński 2024, 182). At

the beginning of September, victualling activities proceeded smoothly, but very soon with the advance of the German army, bombardments paralyzing both the capacity of communication routes and destroying rolling stock and manufacturing centers, as well as piling up difficulties with communications, by the end of the first decade of September, the ability of the Warsaw intendant's office to victual armies fighting in the field was almost completely reduced (Jasiński and Wesołowski 2023, 233-236)).

September 3rd, 1939. Commander-in-Chief Edward Smigly-Rydz ordered Minister of Military Affairs Maj. Gen. Tadeusz Kasprzycki to organize the defense of the middle Vistula River, including Warsaw. This included securing the city also in terms of the intendant. And all this in a situation of enormous chaos, which consisted of the ordered evacuation to the east of civilian and military authorities, as well as institutions, hospitals, etc., with the simultaneous buildup in the city of manpower from military units that had been broken up in the course of fighting and retreating, as well as civilian refugees seeking refuge in the capital.

At the beginning of the second decade of September, the Army "Warsaw" of Maj. Gen. Juliusz Rommel, which was formed to defend the capital region, had about 180,000 soldiers in supply. At that time it had the following supplies accumulated by the intendant's organs: rusks, tinned meat, tinned coffee, cigarettes and salt were estimated at 600 thousand servings; bread flour, together with rye, was estimated at 2,500 tons; thanks to daily deliveries of cattle, the number of livestock ranged from 170 to 500 head, and wounded horses from 200 to 500 head; the amount of groats, flour for seasoning was estimated at 150 tons, and rice at 500 tons; sugar in the depot at Jagiellońska Street 56 was 300 tons, and 500 tons in the Prague port depot; fresh lard and canned smoked pork fat were about 150 tons, plus 100 tons of bacon (Jasiński and Wesołowski 2023, 240). It is estimated that with the transport immobilized at the Warsaw railroad stations, the accumulated supplies could have allowed, under ideal conditions, to provide food for the army for about 30-40 days.

The food supply situation for the civilian population was much worse. Preparations undertaken by the Warsaw Municipal Board before the war were not developed on a large scale, although even so, against the background of other large agglomerations, activities in this regard were undertaken as early as June 1939, and not, for example, as in Vilnius, only in mid-September 1939, when the defensive war was already de facto lost. Purchases of meat, fats, and coal were then begun. The population was ordered to stockpile food for several weeks of fighting. However, the largest warehouses and stores were outside the control of city officials, managed by cooperatives and private individuals.

In the first days of fighting, apart from the rise in prices and long queues of the population standing for necessities, there were no problems with food availability. On September 5th, the Capital's Social Self-Help Committee was established. The Purchasing Section, operating within its framework, efficiently distributed to the

neediest population products received from the City Supply Department or from donations and subsequent requisitions (Rydzewska 1970, 49-50). At the same time, the Warsaw Workers' Social Welfare Committee was also established, which, among other things, was to provide for the care of children and workers' families and to carry out work related to supplying the population with necessities. In view of the impossibility of printing and allocating supply cards, the distribution of rationed goods was handled primarily by the then-created block organizations of the Anti-Aircraft Defense, working closely with the relevant organizational cells of the city. In addition, ad hoc kitchens were organized in the gates of houses using spirit and kerosene machines, on which soups and other dishes were cooked (Milewski 1941, 56).

On September 8th, the first German troops arrived near Warsaw. After unsuccessful attempts to capture it on the march, operations were launched to encircle the city, which interrupted the previous possibility of supplying the city from outside. At the same time, the Germans carried out intensive aerial bombardments and increased artillery fire with each passing day, leading to numerous fires in warehouses, processing plants, bakeries, and stores, significantly reducing both military and civilian food supplies. The imminent threat from German troops caused many private owners to close their stores. With an acute shortage of transportation and the concentration of many supplies in right-bank Warsaw's Praga district, this posed quite a logistical challenge. Therefore, in the situation of the city's underdeveloped victualling apparatus, by the end of the first decade of September, the civilian population in the center of the city began to experience food shortages. This was met with an immediate reaction from the authorities and an order to open stores under the threat of forcible seizure, but also to carry out forced requisitions. Military transport columns drove day and night to decentralize the supplies they had and support the city authorities in this regard as well.

Despite a temporary improvement in the situation, the supply difficulties of both the combatants and the civilian population deepened. This prompted the commander of the "Warsaw" Army to convene a briefing with commanders and the mayor of the city of Warsaw, Stefan Starzynski, who had been acting as Civil Commissioner since September 8th. During the meeting, it was decided to reduce food standards for the army by half with regard to bread and meat. It was also decided to introduce strict control and records of food stocks at the disposal of the city and to disclose all food stocks. The responsible body for overseeing this was the Civil Guard. In turn, the Head of Provisioning at the Civil Commissar, established at that time, began working closely with the army from September 12th in organizing transportation, carrying out requisitions, but also relayed the needs of the civilian population, to whom the army began supplying the following from its warehouses: flour, sugar and rice. Faced with a shortage of meat and a surplus of military horses, the army began returning 200 to 300 wounded horses to the slaughterhouse on a daily basis, and the meat thus obtained was distributed to the population through administrative bodies (Bracławski-Herman 1944, 4-5).

In mid-September, city authorities identified increasing incidents of looting and plundering not only of property, but also of food supplies. This procedure, despite resolute counteraction, due to its scale and the thinness of the forces possible to maintain law and order, continued to a limited extent until the fighting ended. However, it did not remain unaffected by the management of supplies. On September 16th, the Civil Commissar issued an order, affecting primarily the immigrant population, to limit the consumption in public eating establishments to one meal a day. This was to be "nutritious soup." Exceeding this standard was punishable by a hefty fine or three months' imprisonment, or even both at once (Płoski 1964, 78). Confectioneries, on the other hand, dispensed tea or black coffee with buns or rusks.

At the turn of the second and third decades of September, changes were once again made in food rations for the army. The largest rations were set for combat troops and the wounded. Reduced access to food was also felt by the civilian population. Huge queues standing in front of food stores did not spread even during smaller German raids, which often resulted in casualties. The issue of water availability was even worse. As a result of days of bombardment and artillery shelling during the defense, the street sewer system was damaged in a total of 586 places. In addition, 406 damages were found in water supply connections to properties. In turn, as a result of direct hits on September 24th on the Filter Station and the City Power Plant that day, the supply of electricity and water to end users in Warsaw ceased completely (Płoski 1964, 410-411). The few wells could not suffice for the civilian population and the army, so water had to be drawn from the Vistula River (Furmański 1945).

In view of the complete encirclement of the city by the German army and the exhaustion of artillery ammunition, persistence in defense in a city of more than a million inhabitants, daily shelled and bombarded from the air, led to further material losses and further casualties of the civilian population, which was increasingly painfully affected by problems of provisions and lack of medicine. For this reason, on the afternoon of September 26, the Warsaw Defense Command decided to stop fighting and begin capitulation talks with the Germans. On September 28, the Polish capital capitulated. A day later, in a proclamation from the commander of the "Warsaw" Army, Gen. Juliusz Rómmel informed the people of Warsaw: "Today, on my order, the army defending Warsaw and Modlin capitulates due to the exhaustion of ammunition, food, and lack of water. [...] Warsaw has done its duty. The war continues and I firmly believe that victory will be on our side" (Płoski 1964, 133). In accordance with the terms of the capitulation agreement, in the following days after taking control of the city, the German authorities proceeded to distribute bread and hot meals to the population.

## Summary

Interwar Poland was a poor country, facing enormous social and economic problems. Therefore, despite the difficult geopolitical position and the growing threat from the German Reich and the Soviet Union, many projects aimed at securing the

state and its citizens were implemented slowly and inadequately. Unlike the solutions introduced in the German Reich, the issues of problems related to providing provisions for the Polish civilian population during emergencies and war, although accurately diagnosed by the authorities, despite the measures implemented, were not fully and systemically resolved in time. Actions taken by local authorities in the last weeks before the explosion only partially ensured the food security of the population. In Warsaw, it was only thanks to the dedication of thousands of officials led by President Stefan Starzynski, community activists, and also thanks to the supplies accumulated by the army that the specter of starvation was dismissed. In the accounts of the defenders, the food shortage was very often noted. It was pointed out that, although this had a significant impact on the collapse of the morale of the population, the army showed an unwavering will to fight until the end. According to the Polish command, however, further defense was pointless. Faced with a shortage of artillery ammunition, hopes for outside help, and the situation of the civilian population deteriorating with each passing day due to German bombardments and problems with provisions, the Warsaw Defense Command finally decided to capitulate. The issue of the city's victualing was therefore one factor, though certainly not the key one, under whose influence Warsaw capitulated on September 28th, 1939. However, if there was still a political and military sense to the fighting, the issue of ensuring the city's victualling would have been the factor that determined the possibility and length of its duration.

## References

**Bracławski-Herman, Jan.** 1944. *Relacja szefa Oddziału IV Armii "Warszawa".* Archiwum Instytutu Polskiego i Muzeum gen. Sikorskiego, Ref. B.I.93.

**Dokumenty Sekretariatu Obrony Rzeczpospolitej.** 1938. "Centralne Archiwum Wojskowe." Ref. I.303.13.74.

**___.** 1939. "Centralne Archiwum Wojskowe." Ref. I.303.13.74.

**Furmański, Stanisław.** 1945. "Relacja, Archiwum Instytutu Polskiego i Muzeum gen. Sikorskiego." Ref. B.I.71.A.

**Goebel, Władysław.** n.d. *Zaopatrzenie intendenckie armii Warszawa w czasie od dnia 8 IX 1939 do kapitulacji.* Kolekcja 27.3, ref. 25/6/1/a/1/5a., Archiwum Instytut Józefa Piłsudskiego w Londynie.

**Jasiński, Grzegorz.** 2024. "Plany aprowizacji Wojska Polskiego w chleb na czas wojny w 1939 roku." In *Defensive Wars: Poland 1939 - Ukraine 2022-2023. Monograph*, edited by A. Haruk. Wydawnictwo Akademii Wojsk Lądowych we Lwowie. https://doi.org/10.33402/obv.2024-170-185.

**Jasiński, Grzegorz, and Andrzej Wesołowski.** 2023. "Participation of military logistics services in the provision of food in Warsaw in September 1939"." *Systemy Logistyczne Wojsk* 59 (2): 231-246. https://doi.org/10.37055/slw/186390.

**Łuczak, Czesław.** 1982. *Polityka ekonomiczna Trzecie Rzeszy w latach drugiej wojny światowej.* Wydawnictwo Poznańskie.

**Milewski, Jan Kanty.** 1941. *Obrona Warszawy.* 7.9.39-28.9.39.: Bellona.

**Münkel, Daniel.** 1996. *Nationalsozialistische Agrarpolitik und Bauernalltag.* Campus Fachbuch.

**National Archives.** 1939. "Besondere Anordnungen für die rückwartigen Dienste No. 1." Microcopy T-312, r. 39, Armeekommando 8.

**Płoski, Stanisław.** 1964. *Cywilna obrona Warszawy we wrześniu 1939.* Państwowe Wydawnictwo Naukowe.

**Prezydenta Rzeczypospolitej.** 1938. "Rozporządzenie Prezydenta Rzeczypospolitej z dnia 22 II 1938 r." Dz. U. RP nr 13, poz. 89.

**Rodziewicz, Dariusz.** 2022. *Bezpieczeństwo żywnościowe i transport wojenny w polityce obronnej Polski w latach 1919–1939.* Wydawnictwo Naukowe FNCE.

**Rydzewska, Maria.** 1970. "Zaopatrzenia Warszawy w żywność w czasie oblężenia we wrześniu 1939." *Kronika Warszawy* no. 3: 49-59.

**Sulisławski, Mieczysław.** 1939. "Sprawozdanie nt. pracy na stanowisku szefa Oddziału IV Sztabu Naczelnego Wodza." Archiwum Instytutu Polskiego i Muzeum gen. Sikorskiego, ref. B.I.8a/6.

**Urliński, Lech.** 2009. *Polski plan aprowizacji wojennej z września 1939 roku.* Wydawnictwo Adam Marszałek.

**Volkmann, Hans-Erich.** 2003. *Ökonomie und Expansion.* Oldenbourg.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# PKK's Drone Attacks within the Perspective of Learning Organisation and Türkiye's Counter Reaction

**Assoc. Prof. Cenk ÖZGEN, PhD***
**Assoc. Prof. Dr. Selim KURT, PhD****

*Giresun University, Faculty of Economics and Administrative Sciences, Department of Political Science and Public Administration, Giresun, Turkey
e-mail: cenk.ozgen@giresun.edu.tr
ORCID ID: 0000-0002-8583-6194
**Giresun University, Faculty of Economics and Administrative Sciences, Department of Political Science and Public Administration, Giresun, Turkey
e-mail: selim.kurt@giresun.edu.tr
ORCID ID: 0000-0002-0462-5791

## Abstract

PKK's methods used in its terrorist attacks targeting Türkiye have been observed to transform over time. This transformation is influenced by other actors with whom it interacts in its environment and adopts their forms of action. When this interaction is considered from a theoretical perspective, it would be correct to describe the PKK as a "learning organisation". One of the concrete examples of the reflection of the interaction with different actors on the PKK is the organisation's tendency to use drones, largely influenced by ISIS. Records show that drones played an important role in the actions carried out by the organisation. On the other hand, the PKK's start of drone-based actions has resulted in Türkiye increasing its investments in anti-drone systems and using such solutions extensively. The current trend shows that Türkiye has developed and, in parallel with the dynamic structure of the threat, is going to place emphasis on hybrid solutions in the coming period.

**Keywords:**
Learning Organisation; Terrorism; PKK; Drone; Anti-Drone.

**Article info**
Received: 3 April 2025; Revised: 2 May 2025; Accepted: 19 May 2025; Available online: 27 June 2025

Citation: Özgen, C. and S. Kurt. 2025. "PKK's Drone Attacks within the Perspective of Learning Organisation and Türkiye's Counter Reaction. *Bulletin of "Carol I" National Defence University*, 14(2): 93-113. https://doi.org/10.53477/2284-9378-25-18

The fight between Türkiye and the Kurdistan Workers' Party (PKK) terrorist organisation has been going on for nearly 40 years. It is clear that the PKK, which is considered a terrorist organisation by many states, as well as Türkiye, is one of the most dangerous organisations on both a regional and global scale. Undoubtedly, the PKK's military-technical capabilities have an undeniable role in defining it as such a dangerous organisation. The ability of the organisation to adapt to the changing structure of the combat environment is decisive in obtaining these capabilities. It is possible to see the traces of this change in the change in tactics, techniques and procedures applied by the organisation during the conflict process. For example, the organisation, which took good advantage of the authority gap in Iraq during the First Gulf War, increased both the number and destructiveness of its actions in Türkiye with the weapons and ammunition it seized. Similarly, the PKK, which entered into a fight against the Islamic State of Iraq and the Levant (ISIS) terrorist organisation, which emerged from the authority gap in Iraq, has achieved significant gains as a result of this interaction. It is possible to see the reflections of these gains in the PKK's emphasis on the use of remote-controlled mines and hand-made explosives in its actions, and in its practices during the conflict, known as Trench Operations in Türkiye, which includes combat in residential areas due to their physical and human conditions. Another outcome of the interaction with ISIS is the increase in the use of drones in recent years. So much so that the PKK, seeing the military potential of drones in its fight against ISIS, turned to this technology and began to use it widely in its actions in a short time.

The process described above is a clear indication that the PKK, as an organisation, has learned from the events unfolding around it and from other actors. It is accepted that the phenomenon of learning, which in its simplest form can be defined as a process that causes changes in behaviour, is valid for terrorist organisations as well as commercial organisations. At this point, it is certain that the PKK, which applies the knowledge it has acquired in the field, is also a learning organisation. On the other hand, the history of war is, in a sense, the history of precautions and countermeasures. Considering this fact, it is a natural course of action for Türkiye to take precautions against the increasing drone attacks of the PKK. As a matter of fact, Türkiye's practices in the field also coincide with this determination.

On the other hand, although the subject has received intense attention and discussion in the media, it has been assessed in the literature review that it has not received the value it deserves in the academic field. Based on this assessment, it is thought that a study that analyses PKK's drone attacks and Türkiye's search for precautions from a holistic perspective within the framework of the learning organisations approach will fill an important gap in the literature. However, it should be noted that the fact that PKK's drone capabilities specifically and Türkiye's countermeasures to them do not receive sufficient academic attention also poses a problem in terms of reference source supply. In addition, due to the nature of the subject, the content of the sources obtained from open sources is limited, and their confirmation is difficult.

This study reveals PKK's drone capabilities within the framework of the learning organisations approach and discusses Türkiye's search for precautions. In this context, firstly, the learning organisations approach was taken into consideration and its connection with terrorism and the PKK was examined. Subsequently, the PKK's current drone capabilities and the attacks it carried out in the field with these drones were examined. Finally, anti-drone systems in general and Türkiye's capabilities in this field were gone over carefully.

## 1. Learning Organisations, Terrorism and PKK

Acts of political violence, which can generally be described as terrorism, have become a significant threat in today's world. Almost every day, non-state groups in different countries commit acts of violence, many of which can be described as terrorism. The threat of such violence drives ongoing global military activities, and the need for countries to protect themselves against terrorist attacks is the main shaper of the domestic political agenda (Jackson et al. 2005, 2).

On the other hand, changing conditions bring to the fore the importance of terrorist groups' ability to change and adapt. Faced with a challenge to their operational capabilities, terrorist organisations transform the threat they may pose with a restructured form of attack. The ability of terrorist organisations to change their operations effectively over time is inherently linked to their ability to learn (Jackson et al. 2005, 2-3). For this reason, learning is an extremely vital issue for terrorist organisations, too.

Although there are many different definitions, learning is generally defined as "the process of acquiring knowledge through study" (Sun 2003, 154). Learning is also an expression used to describe the process that causes behavioural change. Hence, it is not possible to describe information that does not lead to a change in behaviour as learning. Although there may be many reasons that lead to changes in behaviour, it is desired that the changes that occur as a result of learning are natural, desirable and repeatable in different situations. From this perspective, it is possible to say that learning organisations are organisations that have the ability to change their behaviour (Demir 2008, 58-59). It can be said that learning organisations are organisations that undergo a process of acquiring new knowledge or technology that a group uses to make better strategic decisions, improve certain tactics and implementation skills, and increase the chances of success in their activities. In short, learning is change aimed at improving the performance of a group (Jackson et al. 2005, 9).

When explaining human behaviour, especially behaviour that violates social norms or laws, sociologists often resort to learning. In fact, learning is often reduced to specific theories that go by various names, such as differential association,

conditioning-reinforcement, or social learning. The most well-known of these types of works was carried out by Ronald L. Akers. Akers, who started by reformulating Sutherland's differential association principles within the framework of operant conditioning in the 1960s, further expanded his studies over the years and integrated them with the concepts of indirect, social, non-social and self-reinforcement and named them "Social Learning Theory". Akers's theory is one of the most frequently used theories in criminology and has been applied to a wide range of deviant and criminal behaviours (Akers and Jensen 2003, 1; Akers 1999, 59; Akins and Winfree 2017, 135; Martin 2017, 79). The basic assumption of Akers's theory is that social learning is the primary process that connects social structure to individual behaviour. Its basic proposition is that differences in social structure, culture and the positions of individuals and groups in the social system explain differences in crime rates, mainly through social learning variables. According to Akers, environments that produce deviance have an impact on individual behaviours through the operation of learning mechanisms (Akers 2009, 322).

Much of the existing literature on the learning organisation relates to private sector organisations. However, in recent years, it has been observed that criminal behaviour and terrorist organisations have also been subject to this theory (Garavan 1997, 18). Because, despite the fundamental differences between them, terrorist groups are also organisations. To be successful, they must change, and to change effectively, they must learn. Because they operate in highly volatile environments, it is essential for them to apply what they have learned at the institutional level to survive (Jackson et al. 2005, 9-10).

A terrorist group's ability to learn at the organisational level can make it both more effective and more capable of surviving in hostile environments. If a group can learn successfully, they can develop, improve, and use new weapons or tactics to change their abilities over time. It can improve the skills of its members so that they can better apply their existing weapons or tactics. It can collect and use the intelligence information needed to conduct its operations effectively. It can thwart countermeasures and increase its chances of surviving efforts to destroy it. It can preserve the abilities it has developed even if individual group members are lost (Jackson et al. 2005, 17-18).

Essentially, academic interest in learning about terrorist organisations has predictably increased following the September 11 attacks. At this point, it can be said that the studies largely focus on the Al Qaeda terrorist organisation, which is the perpetrator of this attack, and include issues such as the leadership structure of the terrorist organisation, tactical units, recruitment, training, vision, organisational identity, organisational design and action methods (Demir 2008, 62). On the other hand, it is certain that the PKK, whose official establishment dates back to 1978 and is one of the most dangerous terrorist organisations in its region, has been significantly affected by this global wave of terrorism led by Al Qaeda. In this regard, Özcan

pointed out three factors that ensure the survival of the PKK, which has existed for a long time. The first of these is external support and safe havens; secondly, there is a leadership that is compatible with the cultural norms of the society and the region, and lastly, the organisation's capacity to adapt to the political ecosystem, that is, being a learning organisation. As Özcan points out, the PKK, like all other terrorist organisations, is a "learning organisation" and generally manages to learn from what is happening around it (Özcan 2011).

## 2. PKK's Drone Capabilities and Attacks

### *2.1. A Look at PKK's Drone Capabilities*

Although it is not reflected much in public opinion, the association of the PKK with drones is not a new phenomenon for the Turkish security bureaucracy. The terrorist named Serhat Taysi, a PKK member who went to the police station in Konya in 2007 and surrendered, shared in his statement that the organisation was trying to obtain drones and was preparing to take action against fixed and moving targets with them (Habertürk 2007). Although there is no record of the PKK taking action with such tools in those years. However, this statement shows that the organisation's interest in drones is not today's topic. The general trend on this issue is that the PKK's search for attacks using drones started in 2003-2004 (Erdem 2021).

On the other hand, although its history dates back to the early 2000s, it can be said that what created real awareness about drone technologies for the PKK was the Syrian branch of the organisation, the Democratic Union Party (PYD), observing ISIS's ability to use such tools effectively. Namely, Türkiye has gained serious momentum in the field of defence industry and with this; Developing Unmanned Aerial Vehicle (UAV) capabilities, increasing close air support platforms in terms of quantity and quality, ending foreign dependency on ammunition, building new fortified police stations, and starting to carry out the fight against terrorism entirely by professional units have greatly limited the PKK's capacity to take action (Kasapoğlu and Kırdemir 2019, 3). The organisation, which suffered a high number of militant losses as a result of the domestic and cross-border military operations carried out by the Turkish Armed Forces (TAF) and whose mobility in rural areas came to a halt, turned to drones, which it sees as a relatively risk-free and cost-effective means of action, as a way out. In this context, PKK's attacks using drones began to appear in the Turkish media for the first time in 2016 (Şafak 2016). It was after 2018 that the attacks intensified and became systematic. The attacks carried out in different parts of Şırnak on 10 November 2018, which coincided with the 80th anniversary of Atatürk's death, can be considered a milestone in this respect (Habertürk 2018).

Drones used by the PKK are divided into two types: rotary-wing, multicopter type and fixed-wing, glider type. First of all, it should be noted that these vehicles have completely different flight mechanics and operational planning requirements due to

their designs. Analyses based on open-source intelligence data in the organisation's inventory reveal that there are DJI Phantom, DJI Mavic and DJI Matrice 600 model rotary-wing and RQ-20 Puma, X-UAV Talon model fixed-wing drones (Kasapoğlu and Ülgen 2021, 29-30). Except for the RQ-20 Puma, which was developed for the United States (US) Army, all of the models listed are of Chinese origin and are platforms designed primarily for civil/commercial use. As the X-UAV Talon example shows, it is possible to purchase such platforms from electronic commerce sites without any restrictions and at very reasonable prices, such as approximately 400 dollars (RCDrone 2024). Naturally, these drones sold online do not contain payloads such as weapons or explosives (Sims 2018, 97). However, these platforms can be made suitable for use in terrorist acts by integrating subsystems, which can be easily obtained commercially from all over the world, under limited workshop conditions and without the need for very high technical expertise (Mevlütoğlu 2018). In this context, it is noteworthy that a study conducted at Louisiana State University revealed that a "handmade" drone, which has a payload capacity of approximately 3 kg and can stay in the air for up to 10 minutes, can be produced at a cost of less than $ 2,500 using completely off-the-shelf commercial products (Price 2018, 2). Undoubtedly, the PKK also benefits from these opportunities. Additionally, it should be noted that the organisation receives information, training and logistical support from some non-state actors and foreign intelligence services in the region, which are covered in detail in the first section.

It is noteworthy that in the early periods when the PKK started its drone-based actions, it used rotary-wing, relatively simple models, but in the following period, it also turned to fixed-wing platforms that offer higher payload capacity and range values (Kasapoğlu and Kırdemir 2019, 3). Another notable trend in this field is the use of platforms that do not require remote control and that fly autonomously according to preloaded coordinates of the target for navigation purposes. It is stated that jammers, which interrupt/confuse the data connection between the remote control unit and the drone, are largely ineffective against these platforms, which are observed to use the multi-channel and frequency hopping capable Global Navigation Satellite System (GNSS) technology (Aksan, Sevin and Karaahmetoğlu 2021).

PKK uses drones in general; they are used for reconnaissance-surveillance, target determination and attack purposes. While reconnaissance-surveillance flights are mostly carried out for intelligence gathering, damage assessment and video recording for propaganda purposes, flights for target determination are carried out to direct explosive-laden vehicles to the desired point and to arrange mortar and rocket fire. Vehicles preferred for attack flights are used to release free-falling ammunition to the target with a hand-made release mechanism from a certain altitude, or to dive into the target and destroy it with an explosive carried in the role of a direct hit (kamikaze) drone. It is observed that ammunition such as modified rifle grenades, mortar bullets, rockets or grenades, which fall into the improvised explosive (IED) category, are mostly used in drone attacks. For example, it is a common practice to

attach wings on the back of badminton balls to 40 mm rifle grenades to ensure a more stable fall and increase the hit rate on the target (Cancian 2021).

The recorded attacks show that the organisation targets public buildings and commemorative events, as well as military units and bases (Doğan and Küçük 2021, 7). When the timing of the actions taken against the specified targets is examined, it immediately draws attention that the organisation is seeking to launch simultaneous attacks at different points (Şen 2018). There is also data that the "saturation attack" tactic, which is based on saturating the air defence system and neutralising it, was tried (TRT Haber 2021). It seems that the attacks carried out so far have been somehow foiled by the security forces or have resulted without causing serious casualties. However, the positivity of the balance sheet should not be interpreted as the threat being at a low level. On the contrary, the PKK attaches great importance to improving its capacity regarding aerial platforms in general and drone technologies in particular. Murat Karayılan, the head of the PKK's military wing, People's Defence Forces (HPG), declared 2018 as the "year of aviation" for the organisation, which is a clear indication of the importance given to drones and the intention to take action with these tools (Bural 2021). As emphasised above, when discussing the use of GNSS-based drones, the PKK is seeking to access solutions that can bypass anti-drone systems. The threat from drones will inevitably increase in parallel with the new capabilities to be obtained in this field. When performing a threat analysis, it should be taken into consideration that these tools can be used for critical infrastructures in addition to the existing target scale.

Finally, the intensification of the PKK's actions with drones indicates that a certain capacity has been developed in terms of pilot training and subsystem supply chain. As a matter of fact, it is stated that the organisation, which wants to improve its capacity to take action with aircraft, established a "drone academy" in Mahmur Camp, which is under its control in the north of Iraq, and turned it into a production centre (Orakoğlu 2021). The PKK's unit responsible for drone activities is known as the Delal Amed Air Defence Force. The unit, named after Hülya Eroğlu, codenamed Delal Amed, a member of the PKK Five Executive Council, who was in the red category on the list of wanted terrorists of the Ministry of Internal Affairs and was neutralised in an operation carried out in the Şırnak Bestler Dereler Region on November 2, 2017, monitors the drone actions carried out by the organisation (Bural 2021).

### *2.2. PKK's Drone Attacks Targeting Türkiye*

It is known that the PKK has used various types of drones in its actions targeting Türkiye since 2016. For this reason, it is possible to say that the drone threat to Türkiye is increasing day by day. In this context, it is extremely important to discuss the prominent drone attacks carried out by the PKK against Türkiye, both within the country and in its immediate surroundings, in terms of revealing the dimensions of this threat.

The organisation appears to have gained expertise in the use of weaponised commercial unmanned aerial vehicles, especially with the help of its Syrian sister organisation, the People's Defence Units (YPG). In 2016, Türkiye seized two RQ-20 drones from the PKK, allegedly taken from northern Syria. According to Turkish experts, the PKK started using drones in its operations in 2016. The first attack in this context took place in Hakkari on October 12, 2016. A hand grenade-trapped drone used by the PKK was shot down while trying to land on a military unit. It was also claimed that attacks were carried out against Turkish bases in Iraq in 2017 with armed drones (En Son Haber 2016; Zwijnenburg 2023, 17). In 2017, two more attacks carried out by the terrorist organisation using drones were recorded. Regarding the first of these, in the statement made by the Ministry of Internal Affairs: "On Wednesday, August 30, 2017, in the Hakkari-Şemdinli District, Derecik Town, Biz Tepe Base area, as a result of the fire opened by the elements carrying out an operation in the field, a drone (6 propellers, capable of releasing explosive materials with a spring system, 130 cm between two wings) belonging to the terrorist organisation, coming from Iraqi territory and considered to be preparing for an attack, was hit." (Ministry of Internal Affairs 2017a) In the second one, it was reported that a drone loaded with grenade launcher ammunition was seized in the Doğu Beyazıt district of Ağrı on November 12, 2017 (Erdem 2021).

The number of attacks recorded in 2018 was three. In this context, on November 10, 2018, the terrorist organisation targeted the November 10 ceremonies in Şırnak and attacked ten different points, including the governor's office, with drones carrying C-3 and C-4 explosives (Yeni Şafak 2019). Regarding another attack, according to the information made on the official Twitter account of the General Staff, on May 3, 2018, the drone belonging to the terrorists approaching the Güven Base Region in Zap in the north of Iraq from the south was shot down with anti-drone weapons and neutralised (Anadolu Ajansı 2018).

There were six attacks recorded in 2019. In the first of these, an attack was carried out on Ercüment Turkmen Barracks in Silopi on February 24, 2019, with drones loaded with 60 mm mortar bullets. It was stated that a large-scale investigation was initiated regarding the attack, which reportedly resulted in no loss of life (Yeni Şafak 2019). In the second one, it was announced that twelve attacks carried out by the terrorist organisation YPG/PKK with drones launched from the east of the Euphrates in two consecutive weeks in March 2019 were prevented by the Turkish Armed Forces. It was announced that the targets of these attacks, which were carried out with drones targeting domestic base areas and directed from terrorist bases deep in Syria, were the Turkish Armed Forces elements in Şırnak's Silopi, Gaziantep's İslahiye, Şanlıurfa's Suruç and Birecik districts. It was reported that all of the attacks were prevented by the security forces with anti-drone weapons and various weapon systems, and there were no casualties (Özer 2019). In the third attack, it was announced that the IED-laden drone belonging to PKK terrorists, located in the Dilucu Customs Directorate area, which is the Nakhchivan border gate, was detected and neutralised

by the Aselsan Milkar 5S anti-drone system. The incident took place on June 21, 2019, around 12.30, at the Dilucu Border Gate in the Martyr Bülent Aydın Border Team Patrol Command's responsibility area of the Aralık district. It was stated that the explosive-laden drone, which was determined to be sent by PKK terrorists, was detected and neutralised by the Aselsan Milkar 5S anti-drone system located in the Dilucu region under the responsibility of the 5th Border Regiment Command (Aydın 2019). Another attack in 2019 took place in Batman on December 4, 2019. The bomb-laden drone, which took off from the village of Muzen in the town of Amude in Syria, targeted the section where the oil boilers were located at the Tüpraş Oil Refinery, and the disaster was averted when the bomb drone exploded 5 meters behind. It was claimed that the fingerprints of Syrian PKK/PYD terrorists were found on the drone (B. Doğan 2022).

So, eight attacks of the terrorist organisation were recorded in 2020, when the attacks increasingly intensified. In this context, the Ministry of National Defence (MSB) announced that PKK terrorists attempted to attack the base area in northern Iraq with two drones on August 20, 2020, and the aircraft in question were shot down. In the statement made by A Haber correspondent regarding the incident, it was said: "The attack attempt was intended to be carried out against Turkish troops in the Şeladize town of Northern Iraq at around 07:00 in the morning. The terrorist organisation PKK attacked with a drone but was unsuccessful. There was no loss of life in the attack attempt with a drone. It was destroyed in the air." Stating that the drones destroyed in the air fell in various areas in the region, the reporter added that the PKK's attack was repelled thanks to the signal jamming system (Takvim 2020).

On the other hand, it was determined that there were twelve attacks recorded in 2021, when the trend of drone attacks increased. In the first of these, the Ministry of National Defence announced that a drone used by terrorists to attack Turkish Armed Forces elements was destroyed on May 11, 2021, during the ongoing Claw-Lightning and Claw-Lightning operations in the north of Iraq. In the statement, it was noted that the soldiers, who were carrying out search and scanning activities in the Metina region where the Claw Lightning operation was held, noticed a drone coming towards them and opened fire with machine guns, and it was shot down before it could reach its target (NTV 2021a). Regarding another attack, Diyarbakır Governorship reported that an attempt was made to attack the 8th Main Jet Base Command with drones. In the statement made by the Governorship, it was stated that an attempt was made to attack Diyarbakır 8th Main Jet Base Command with drones at around 00.30 on May 18, 2021, and that the drone used in the attack was shot down and there were no casualties at the base. Regarding the issue, the Minister of Internal Affairs at the time, Süleyman Soylu, also made a statement: "An attempt was made to attack a military facility in Diyarbakır with two drones, the drones were neutralised and there were no casualties." he said (Euronews 2021). On the other hand, it was announced that a similar attack attempt occurred in Batman and Şırnak provinces on May 21, 2021, just three days after the attack attempt against Diyarbakır

2nd Air Force Command. Members of the terrorist organisation PKK attempted to attack Batman Airport Command with three and Şırnak 23rd Gendarmerie Border Division Command with two explosive-laden drones. As the security forces noticed the situation, the drones were shot down in the air (Kaçar 2021). Regarding another attack attempt, in the statement made by the Ministry of National Defence, it was stated that on May 25, 2021, PKK terrorists attempted to attack with a base drone in the Euphrates Shield region, the aircraft in question was shot down, and in the operation carried out at the point where the plane took off, a PKK/YPG terrorist was neutralized (NTV 2021b).

By 2022, it was announced that the terrorist organisation PKK started to target base areas with explosive-laden drones in response to the Claw-Lock operation launched by the Turkish Armed Forces in the north of Iraq. In this context, on May 9, 2022, the PKK tried to attack the base areas of the Turkish Armed Forces with drones. The explosive-laden drone approaching the base areas was detected, taken under fire and shot down. On May 5, it was announced that the terrorist organisation PKK tried to attack the base areas with an explosive-laden drone and that the attack attempt was prevented by members of the Turkish Armed Forces (CNN 2022). In another attack attempt in 2022, it was reported that the Turkish Armed Forces' Bamerne base in Duhok was attacked with drones. It was announced that an attack was carried out with two drones on the Turkish Armed Forces' military base in Bamerne in the morning hours of July 22, there was no loss of life due to the attack, one of the drones was shot down by fire from the base, and the other fell by itself. Although no one claimed responsibility for the attack, it is thought to have been carried out by the PKK (Cumhuriyet 2022).

On the other hand, it was reported that PKK's bomb drones were shot down in the Claw-Lock Operation region on September 11, 2023. It was stated that PKK terrorists, for whom the USA gave drone training, attempted to attack four hills in the Claw-Lock Operation region with nine bomb-laden drones, and these drones were shot down with IHASAVAR and anti-aircraft guns. It was announced that the drones in question took off from PKK camps in the southeast of Metina (Star 2023).

## 3. Anti-Drone Systems and Türkiye

### *3.1. Overview of Anti-Drone Systems*

It can be said that until recently, the capabilities of terrorist organisations regarding aircraft were limited, but cheap and easily accessible civilian drone technology has changed this situation (Chaves and Swed 2020, 31). Terrorist organisations seeking sensational action have discovered the potential of drones and started to use them widely. Nowadays, many terrorist organisations operating in different regions of the world, such as the Middle East, Africa, South America and Southeast Asia have such vehicles in their inventories (Bergen, Salyk-Virk and Sterman 2020). Due to the

ease of procurement, no change in the picture is expected, at least for the foreseeable future, and this shows the need to take precautions and the importance of using anti-drone systems.

Anti-drone systems mean fixed or mobile solutions that detect and neutralise drones by working in coordination with various components (Zmysłowski, Skokowski and Kelner 2023, 459). Although they have the same meaning, definitions such as drone countermeasure systems are also made for such solutions in the literature. In fact, from a doctrinal perspective, anti-drone systems are also included in the low-altitude air defence systems layer, and their design architectures are similar to other air defence systems. As a matter of fact, like all air defence systems, these systems consist of three main components: sensor, command-control and weapon (Meteksan 2020). On the other hand, traditional air defence systems are optimised for the detection, tracking and destruction of large and fast platforms such as aircraft, helicopters and cruise missiles. Technically, it is not possible for these systems to be effective under all conditions against small and slow-flying drones at very low altitudes (Michel 2019, 2). As a result, it can be said that anti-drone technology was developed by taking into account the disadvantages of existing air defence systems, which are inadequate against the increasingly widespread drone threat, and the main distinction between these systems is made based on their potential targets.

Anti-drone systems are divided into three types: land-based, hand-held and UAV-based (Business Research Insights 2024). No matter what category they fall into, these systems neutralise threatening drones; it takes place within a kill-chain, which is listed as detection, diagnosis, tracking and response (4T). In the destruction-chain in question, radar, radio frequency (RF) analyser, electro-optical/infrared camera and acoustic sensor systems are used for detection, diagnosis and tracking stages. There are also solutions where these systems are integrated with each other (Michel 2019, 3). In the reaction phase, which is the last link of the destruction-chain, hybrid systems in which physical-destruction (hard-kill), functional-destruction (soft-kill) or both are used come into play. In this context, in physical-destruction systems, the target is neutralised using kinetic ammunition, while in functional-destruction systems, the target is neutralised by non-kinetic electronic warfare applications (Eshel 2017). Physical-destruction systems include weapons, lasers and networks; RF jamming, GNSS jamming and deception are examples of functional-destruction systems. On the other hand, in some scenarios, such as RF jamming being ineffective against autonomous drones, it is not possible to obtain definitive results by using a single system. Therefore, when taking precautions, such scenarios should be taken into consideration (Sütçüoğlu and Alay 2019, 6-7).

From a military geography perspective, the places where anti-drones are used can be basically divided into two: residential areas and rural areas. First of all, it should be underlined that the areas where it is more difficult to develop countermeasures are the residential ones. Factors such as the presence of multi-storey buildings

with different architectural designs, the intensity of air traffic, the high level of electromagnetic pollution and the abundance of unwanted echoes make it difficult to detect small-sized drones in residential areas (Robin Radar Systems 2021). By taking off from any point in a residential environment with a rotary-wing drone, it is possible to attack targets such as public buildings, general law enforcement stations and meeting places. Unlike in rural areas, what complicates the equation here is the difficulty of creating a destruction chain. The number of potential targets that need to be protected is very high (Doğan and Küçük 2021, 20). Even if anti-drone solutions are deployed sufficiently, none of the detection systems, from radars to acoustic sensors and optical/thermal cameras, work at full capacity in the residential environment, resulting in a shortening of the reaction time and an increased risk of secondary damage (Deschenes 2019, 51). It should also be noted that the risk of collateral damage is a factor that limits the use of solutions based on physical destruction, especially within densely populated civilian settlements.

Regardless of whether they are inside or outside residential areas, vehicles and critical infrastructures in sectors such as transportation and energy are among the high-value targets for drone attacks. For example, passenger aircraft are extremely vulnerable to drone attacks, especially during the take-off/climb and approach/landing phases of the flight. Although manufacturers design aeroplanes to be resistant to bird strikes, there are no tests for a drone entering the engine or hitting the cockpit windshield (Paganini 2016). In this context, it should be noted that tests conducted at the Impact Resistance Laboratory of the University of Dayton Research Institute revealed that even collisions with mini-class drones weighing a few kilograms can cause serious structural damage to passenger aircraft. Moreover, drones that did not carry explosives were used in the tests in question, and the damage was caused entirely by kinetic energy. It is obvious that the threat posed by a drone modified to carry explosives will be much higher. Another example that can be given in this context is refineries. Their vital importance for the maintenance of economic activities and the possibility that interruptions in production processes may have devastating consequences make refineries among high-value targets (Fortem Technologies 2024). The drone attacks that targeted Saudi Aramco's Abqaiq refinery and Hurays oil field on September 14, 2019, causing Saudi Arabia's oil exports to decrease by approximately 60% and causing the Brent oil price to increase by more than 10%, reveal the extent of the threat (The Economist 2019).

### *3.2. Türkiye's Anti-Drone Capabilities*

The start of drone-based actions, performed by terrorist organisations such as the PKK and ISIS, has led Türkiye to focus on developing countermeasures, and has also resulted in the widespread use of anti-drone technologies in the field. In this context, in parallel with the increase in the drone threat, it can be noticed that original solutions are rapidly developed by Turkish defence industry companies and offered to the service of the Turkish Armed Forces and general law enforcement forces. It is considered that anti-drone systems, which are gradually entering the inventory, are

distributed according to the threat level and, accordingly, priority is given to military bases and troops in the field, which are of critical importance in the fight against terrorism. It should also be emphasised that these systems are used to protect critical infrastructures, public buildings, assembly areas and government officials.

It seems that the solutions put into service in the first place are systems that fall into the functional-destruction category and generally use the RF jamming method. However, after a while, the dynamic nature of the threat caused systems that only affect the RF spectrum to become insufficient, resulting in the need to take additional measures. In this regard, the provision of systems that jam GNSS signals or conduct deception attacks to mislead previously entered navigation coordinates can be considered as measures developed based on the change in threat parameters. A similar evaluation can be made for the inventory of physical-destruction systems that use kinetic ammunition. Due to its advantages, it has been observed that the supply trend in recent years has shifted towards solutions that use different prevention methods together.

There is no inventory list shared with the public by official authorities regarding the anti-drone systems used by Turkish security forces. Despite this, it was possible to conduct an inventory study by analysing both the news reported in the media at various times and the statements made by authorised individuals or manufacturing companies. Anti-drone systems found to be used by the Turkish Armed Forces and general law enforcement forces will need to be mentioned further on. It should be noted in advance that there may be systems that are not included in the study because this situation could not be detected even though they are in active use. Likewise, it should be noted that systems that are known to have been developed by Turkish companies, but whose entry into the inventory cannot be confirmed at this stage, and jammers designed to neutralise threats such as IEDs are also excluded from the scope.

The first of the anti-drones in the inventory of Turkish security forces is Aselsan's İHASAVAR system. Standing out with its cost-effectiveness, İHASAVAR has a compact design architecture that can be used by a single soldier, and is basically a gun-type anti-drone system consisting of a backpack and a handheld rifle-like directional antenna equipment. It is stated that İHASAVAR, with an output power of 50 watts, can mix all RF and GNSS-based navigation, data and image transmission frequencies simultaneously (Mehmet 2018). The effective range of İHASAVAR is between 2 and 3 km. The system, which allows the targeted drone to land at its location by cutting off its data connection, can broadcast uninterruptedly for at least 1.5 hours thanks to its rechargeable high-capacity Li-Ion batteries (Haber 2018). Delivery of İHASAVAR to Turkish security forces started in November 2017. There is information in open sources that nearly 1,000 systems were in service at home and abroad as of April 2020 (TR Military News 2020).

Another anti-drone system developed by Aselsan and included in the inventory of Turkish security forces is IHTAR. IHTAR, which has fixed and mobile versions that can be integrated on vehicles and provides uninterrupted 360-degree coverage 24 hours a day in all weather conditions, has a design suitable for the protection of base areas, critical facilities and crowded organisations in urban and rural environments. The basic components of IHTAR consist of ACAR radar, HSY electro-optical system, GERGEDAN jamming/blinding system and command-control system. Additionally, it is possible to integrate different sensors and physical destruction systems into the standard configuration (Aselsan 2022a). IHTAR, which is used to protect critical facilities such as the Presidential Complex, Akkuyu nuclear power plant and TÜPRAŞ refineries in Türkiye, was exported to TRNC, Kyrgyzstan, Niger and Angola as stated (Mehmet 2023).

One of the systems developed by Aselsan against the drone threat is the ŞAHİN 40mm Physical Destruction System. Integrated on a towed trailer with easy deployment and installation features, ŞAHİN performs automatic target detection and tracking with its advanced electro-optical cameras mounted on a stabilised turret and destroys threatening drones with its 40mm MK19 Mod3 Bomb Launcher gun. ŞAHİN's effective range is 700 m, and its ammunition capacity is 64 units. In order to increase the hit rate, ATOM 40mm High Speed Smart Grenade Launcher Ammunition, based on time programmed fuse technology, is used in ŞAHİN (Aselsan 2022b).

Another anti-drone system used by Turkish security forces is Roketsan's ALKA Directed Energy Weapon System. ALKA, a hybrid system, draws attention with its two-layered defence architecture in which functional-destruction and physical-destruction methods are used together. In this architecture, threats detected and tracked by radar and electro-optical systems are first tried to be prevented with an electromagnetic jamming weapon, and if this is not sufficient, a laser weapon is activated. ALKA, whose laser weapon has an effective destruction range of 750 m, can prevent swarm attacks regardless of the number of targets, thanks to the lack of ammunition restrictions. ALKA, which offers lower shooting costs compared to conventional methods, has fixed and mobile versions (Roketsan 2022). A report in the Western media stated that ALKA was deployed in Libya and shot down a Chinese-made Wing Loong II type unmanned aerial vehicle belonging to the United Arab Emirates on August 4, 2019. It should be underlined that the engagement in question was recorded as the first use of a laser weapon in real combat conditions (Timokhin 2019).

Another anti-drone used by the Turkish security forces is the İLTER Drone Detection and Blocking System developed by Boğaziçi Defence Technologies. Essentially, İLTER is the general name of an anti-drone product family that includes various RF and radar-based systems. All systems in this family have

fully automatic target detection and prevention features. Another common feature of the systems in the product family is 24-hour uninterrupted operation and 360-degree protection against multiple drone attacks (Boğaziçi Savunma Teknolojileri 2024). It is stated in open sources that the number of ILTERs delivered to the Turkish security forces as of October 2020 is approximately 350 (Yıldırım 2020). It is known that İLTER, which has a localisation rate of over 90 per cent, has been exported to more than 10 countries with its successful performance in the field (TRT Haber 2023).

Another anti-drone system in the inventory of the Turkish Armed Forces and the General Directorate of Security (EGM) is Harp Arge's DRONE SAVAR. DRONE SAVAR, which is stated to be the first solution in its category developed and produced in Türkiye, is a gun-type anti-drone system that can be used by a single soldier. In general, DRONE SAVAR consists of a backpack carrying electronic systems and batteries, and a rifle-like antenna equipment with a foldable stock and grip for ease of transportation. It is an important advantage that DRONE SAVAR, which has a battery life of 1.5 hours and provides ease of use with its lightness, has Picatinny rails that enable the mounting of different accessories. Azerbaijan is among the known users of DRONE SAVAR (Yıldırım 2017).

One of the anti-drone systems included in the inventory of the Turkish Armed Forces is KALKA, developed by the National Defence. KALKA, which has fixed and mobile versions and can be used in manual or automatic mode according to the operator's preference, provides protection in a circular area of approximately 3 km, depending on geographical conditions. KALKA consists of a detector that acts as a sensor by detecting the RF communication between the approaching drone and the control centre, and a jamming system that ensures functional destruction. KALKA's first export customer was a Russian private sector company that placed an order to protect its own facilities (Haber Aero 2020).

Three different weapon types of anti-drone systems developed by the National Defence have also entered the inventory of the Turkish Armed Forces. In this context, the first of the systems actively used in the field is; it is İHAMIX, with 21 watts of output power. The effective range of İHAMIX, which weighs 4.5 kg and has an operating time of 60-80 minutes, is 1,000-1,500 m. The Picatinny rails on it make it possible to mount various optical sights on the İHAMIX. The output power of another system, İHAMINI, is 15 watts. The effective range of İHAMİNİ, which weighs 3 kg and has an operating time of 60-80 minutes, is 700-1,000 m. İHATİM, which is the smallest of the weapon-type anti-drone systems produced by the National Defence, has an output power of 6 watts. The effective range of İHATİM, which weighs 2.5 kg and has an operating time of 60-80 minutes, is 300-500 m.

## Conclusion

There is no doubt that the PKK is a learning organisation, constantly updating and improving its methods in terrorist acts. It is possible to see the traces of this in the use of drones in the actions taken in recent years, so much so that, in its fight against ISIS in Iraq and Syria, the PKK discovered the potential of drones in an asymmetric combat environment and quickly copied it. As a matter of fact, it is possible to evaluate the increase in the use of drones in their actions after 2016 within this framework.

The PKK's focus on drone-related actions has caused Türkiye, which already has a certain knowledge in anti-drone technologies, to further accelerate its work in this field. Essentially, the process progresses in a spiral of precautions and countermeasures. Namely, while the systems used by the Turkish security forces in the first place were systems that fell into the functional-destruction category and generally used the RF jamming method, the dynamic nature of the threat caused them to become insufficient after a whileand, as a solution, the supply of systems that scrambled GNSS signals or devices that carry out deception attacks to mislead previously entered navigation coordinates has come to the fore. Moreover, the dynamic nature of the threat has led to the inclusion of physical-destruction systems using kinetic ammunition into the inventory after a while, and it is possible to say that, due to their advantages, the supply trend in recent years has shifted towards hybrid solutions that use different prevention methods together.

Undoubtedly, it is important to have advanced anti-drone systems in the inventory in combating the drone threat and studies in this field need to continue. On the other hand, it is not possible to combat the increasing drone threat with purely military-technical solutions, and this does not coincide with the realities of the battlefield. It is also essential to take additional measures against the drone threat posed by the PKK and similar organisations. At this point, it is considered to be of critical importance to cut the organisation's supply chains and destroy the training and production-modification infrastructure.

## References

**Akers, R.L.** 1999. *Criminological Theories.* New York: Routledge.

**___.** 2009. *Social Learning and Social Structure: A General Theory of Crime and Deviance.* New Jersey: Transaction Publishers.

**Akers, R.L., and G.F. Jensen.** 2003. *Social Learning Theory and the Explanation of Crime.* Introduction (pp. 1-8). Edited by R. L. Akersand and G. F. Jensen. New York: Routledge.

**Akins, J.K., and L.T. Winfree.** 2017. "Social Learning Theory and Becoming a Terrorist: New Challenges for a General Theory." In *The Handbook of the Criminology of Terrorism*, edited by G. LaFree and J. D. Freilich (pp. 133-149). West Sussex: John Wiley & Sons, Ltd.

**Aksan, S., S. Sevin, and C. Karaahmetoğlu.** 2021. "PKK'nın yeni saldırılarında 'yabancı istihbarat' izleri." *TRT Haber.* https://www.trthaber.com/haber/gundem/pkknin-yeni-saldirilarinda-yabanci-istihbarat-izleri-585153.html.

**Anadolu Ajansı.** 2018. *Teröristlere ait drone düşürüldü.* https://www.aa.com.tr/tr/turkiye/teroristlere-ait-drone-dusuruldu/1134588.

**Aselsan.** 2022a. *İHTAR anti-drone sistemi.* https://wwwcdn.aselsan.com/api/file/IHTAR_TR-(1)-(1)-(1).pdf.

**___.** 2022b. *ŞAHİN 40mm fiziksel imha sistemi.* https://wwwcdn.aselsan.com/api/file/SAHIN_40mm_TR.pdf.

**Aydın, Ö.** 2019. "Dilucu'ndaki PKK saldırısı drone savar sistemiyle önlenmiş." *Hürriyet.* https://www.hurriyet.com.tr/yerel-haberler/igdir/merkez/dilucundaki-pkk-saldirisi-drone-savar-sistemiy-41252033.

**Balkan, S.** 2019. *Devlet Dışı Silahlı Aktörler Ve Terör Örgütlerinin Yeni Aracı: İHA*. İstanbul: SETA Yayınları.

**Bergen, Peter, Melissa Salyk-Virk, and David Sterman.** 2020. "World of Drones." *New America.* https://www.newamerica.org/future-security/reports/world-drones/.

**Boğaziçi Savunma Teknolojileri.** 2024. *Elektronik harp sistemleri.* https://www.bogazicisavunma.com/.

**Bural, E.** 2021. "Öğrenen örgütler yaklaşımı çerçevesinde PKK terör örgütünün drone ve maket uçak eylemleri." *TERAM.* https://www.teram.org/Icerik/ogrenen-orgutler-yaklasimi-cercevesinde-pkk-teror-orgutunun-drone-ve-maket-ucak-eylemleri-153.

**Business Research Insights.** 2024. *UAV Jammer Market Report Overview.* https://www.businessresearchinsights.com/market-reports/uav-jammer-market-105315.

**Cancian, M.** 2021. "What is the buzz about drones? Evolutionary, not revolutionary." *Modern War Institute.* https://mwi.westpoint.edu/whats-the-buzz-about-drones-evolutionary-not-revolutionary/.

**Chaves, K., and O. Swed.** 2020. "Off the shelf: the violent nonstate actor drone threat." *Air & Space PowerJournal* 34 (3): 29-43.

**CNN.** 2022. *Terör örgütünden 2. maket uçaklı saldırı.* https://www.cnnturk.com/video/turkiye/teror-orgutunden-ikinci-maket-ucakli-saldiri.

**Cumhuriyet.** 2022. *Irak'ın kuzeyinde TSK üssüne 'iki drone saldırısı' iddiası: Dronelar düşürüldü.* https://www.cumhuriyet.com.tr/turkiye/irakin-kuzeyinde-tsk-ussune-iki-drone-saldirisi-iddiasi-dronelar-dusuruldu-1960832.

**Demir, C.K.** 2008. "Öğrenen örgütler ve terör örgütleri bağlamında PKK." *Uluslararası İlişkiler* 5 (19): 57-88.

**Deschenes, P.** 2019. "The rise of the drones: technological development of miniaturised weapons and the challenges for the Royal Canadian Navy." *Canadian Military Journal* 19 (2): 51-56.

**Doğan, B.** 2022. "Tel Rıfat Münbiç ve Kobani Türkiye için tehdit: Dört yılda 81 saldırı önlendi." *Yeni Şafak.* https://www.yenisafak.com/gundem/tel-rifat-munbic-ve-kobani-turkiye-icin-tehdit-dort-yilda-81-saldiri-onlendi-3893038.

**Doğan, K., and F.M. Küçük.** 2021. *Türkiye'ye Yönelik Drone Tehdidi, PKK Terör Örgütü ve İran'ın Milis Örgütleri.* Ankara: Defence Turk.

**En Son Haber.** 2016. *PKK'lı teröristler drone ile saldırı girişiminde bulundu.* https://www.ensonhaber.com/ic-haber/pkkli-teroristler-drone-ile-saldiri-girisiminde-bulundu-2016-10-12.

**Erdem, A.K.** 2021. "Drone saldırıları PKK'nın yeni stratejisi mi? Uzmanlar: Örgüt drone saldırılarını yaygınlaştırmayı ve şehirlere yaymayı planlıyor." *Independent Türkçe.* https://www.indyturk.com/node/363106/haber/drone-sald.

**Eshel, T.** 2017. "U.S. Army to evaluate counter-drone gun system." *Defence Update.* https://defense-update.com/20170314_drs_c-uas.html.

**Euronews.** 2021. *Diyarbakır Valiliği: 8. Ana Jet Üs Komutanlığına maket uçaklarla saldırı girişiminde bulunuldu.* https://tr.euronews.com/2021/05/19/diyarbak-r-valiligi-8-ana-jet-us-komutanl-g-na-maket-ucaklarla-sald-r-girisiminde-bulunuld.

**Fortem Technologies.** 2024. *High Value Targets.* https://fortemtech.com/solutions/energy-industrial/.

**Garavan, T.** 1997. "The learning organisation: a review and evaluation." *The Learning Organisation* 4 (1): 18-29. https://doi.org/10.1108/09696479710156442.

**Haber Aero.** 2020. *Rusya yerli dronesavar KALKA'ya talip oldu.* https://www.haber.aero/savunma/rusya-yerli-dronesavar-kalkaya-talip-oldu/.

**Haber, Donanım.** 2018. "Şüpheli İHA'lar İHASAVAR ile durduruluyor." https://www.youtube.com/watch?v=ntKWRo-Ycww.

**Habertürk.** 2007. *Bombacının itiraflarından.* https://www.haberturk.com/gundem/haber/24356-bombacinin-itiraflarindan.

**___.** 2018. *Teröristler Şırnak'ta 8 model uçakla saldırı düzenledi.* https://www.haberturk.com/teroristler-sirnak-ta-8-model-ucakla-saldiri-duzenledi-2216071.

**Jackson, B.A., J.C. Baker, K. Cragin, J. Parachini, H. R. Trujillo, and P. Chalk.** 2005. *Aptitude for Destruction: Volume 1, Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism.* Santa Monica: RAND Corporation.

**Kaçar, H.** 2021. *Şırnak ve Batman'da askeri tesise saldırı girişimi!.* https://www.sabah.com.tr/gundem/2021/05/20/son-dakika-batmanda-askeri-tesise-saldiri-girisimi.

**Kasapoğlu, C., and B. Kırdemir.** 2019. *Terör Tehdidinde Yeni Boyut: Drone Saldırıları ve Türkiye'nin Milli Güvenliğine İlişkin Gelişmeler.* İstanbul: EDAM.

**Kasapoğlu, C., and S. Ülgen.** 2021. *In the Shadow of Guns: Armament Trends of the PKK and YPF Terrorist Network.* Istanbul: EDAM.

**Martin, G.** 2017. *Terörizm: Kavramlar ve Kuramlar.* Translated by İ. Çapçıoğlu and B. Metin. Ankara: Adres Yayınları.

**Mehmet, F.** 2018. "İHASAVAR anti-drone sistemi." *Defence Turk.* https://www.defenceturk.net/ihasavar-anti-drone-sistemi.

___. 2023. "Drone avcısı İHTAR İHA önleme sistemi 4 ülkeye ihraç edildi." *Defence Turk*. https://www.defenceturk.net/ihtar-iha-onleme-sistemi-4-ulkeye-ihrac-edildi.

**Meteksan.** 2020. *Counter Drone Systems: Tailor-Made System Solutions Based on Open System Architecture.* https://www.meteksan.com/en/yayinlar/articles/counter-drone-systems-tailor-made-system-solutions-based-on-open-system-architecture.

**Mevlütoğlu, A.** 2018. "10 Kasım bombalı İHA saldırıları üzerine bazı notlar." *Siyah Gri Beyaz.* https://www.siyahgribeyaz.com/2018/11/10-kasm-bombal-iha-saldrlar-uzerine-baz.html#more.

**Michel, A.H.** 2019. *Counter-Drone Systems. New York.* New York: Centre for the Study of the Drone.

**Ministry of Internal Affairs [İçişileri Bakanlığı].** 2017a. *Terörle mücadele bülteni.* https://icisleri.gov.tr/kurumlar/icisleri.gov.tr/Basin/2017/A%C3%A7%C4%B1klamalar/04.09.2017.pdf.

___. 2017b. *PKK/KCK terör örgütünün Suriye kolu: PYD-YPG.* https://www.icisleri.gov.tr/kurumlar/icisleri.gov.tr/IcSite/strateji/deneme/YAYINLAR/%C4%B0%C3%87ER%C4%B0K/pyd_tr_fr.pdf.

**NTV.** 2021a. *Irak'ın kuzeyinde teröristlerin Mehmetçik'e saldırı amaçlı kullandığı maket uçak düşürüldü.* https://www.ntv.com.tr/turkiye/pkkdan-maket-ucakla-saldiri-girisimi,CsfMI63T70arVK2q4r1QGw#.

___. 2021b. *Fırat Kalkanı bölgesine maket uçakla saldırı girişimi.* https://www.ntv.com.tr/turkiye/firat-kalkani-bolgesine-maket-ucakla-saldiri-girisimi,6UDpdGZkB0ST_dOHF6ldQw.

**Orakoğlu, B.** 2021. "PKK'nın Mahmur Kampı'nda sözde drone akademisinin faaliyetlerine dikkat." *Yeni Şafak.* https://www.yenisafak.com/yazarlar/bulent-orakoglu/pkknin-mahmur-kampinda-sozde-drone-akademisinin-faaliyetlerine-dikkat-2058702.X.

**Özcan, N.A.** 2011. "Do you think the PKK is stupid?" *TEPAV.* https://www.tepav.org.tr/en/blog/s/2899.

**Özer, S**. 2019. "Suriye'nin kuzeyinden son iki haftada "drone"lu 12 saldırı." *Anadolu Ajansı.* https://www.aa.com.tr/tr/turkiye/suriyenin-kuzeyinden-son-iki-haftada-dronelu-12-saldiri/1413905.

**Paganini, P.** 2016. "A small drone hit a British Airways plane over the Heathrow Airport." *Security Affairs.* https://securityaffairs.com/46442/security/drone-hit-british-airways-plane.html.

**Price, R.** 2018. "Build Your Own Sprayer Drone." *LSU AgCenter.* https://www.lsuagcenter.com/~/media/system/9/b/e/f/9bef3661b2786c2d6b635f0a7c8870fe/p3633_buildownsprayerdronefactsheetnew_rch0718rpricepdf.pdf.

**RCDrone.** 2024. *X-UAV Talon EPO 1718mm Wingspan V-tail White Version FPV Flying Glider RC Model Aeroplane.* https://rcdrone.top/products/x-uav-talon-epo-1718mm?_pos=2&_psq=talon&_ss=e&_v=1.0.

**Robin Radar Systems**. 2021. *Why Drone Radar Needs to Perform in Urban Environments to Tackle Today's Threat.* https://www.robinradar.com/press/blog/why-drone-radar-needs-to-perform-in-urban-environments-to-tackle-todays-threat.

**Roketsan.** 2022. *ALKA NEW (Network Enabled Weapon) ağ yetenekli silah.* https://www.roketsan.com.tr/tr/urunler/alka-new-ag-yetenekli-silah.

**Sims, A.** 2018. "The Rising Drone Threat from Terrorists." *Georgetown Journal of International Affairs* Vol. 19: 97-107.

**Star.** 2023. PKK'nın bombalı dronları düşürüldü! ABD İHA'sıyla saldırdılar. https://www.star.com.tr/dunya/pkknin-bombali-dronlari-dusuruldu-abd-ihasiyla-saldirdilar-haber-1811381/.

**Sun, H.C.** 2003. "Conceptual clarifications for 'organizational learning', 'learning organization' and 'a learning organization'." *Human Resource Development International* 6 (2): 153-166.

**Sütçüoğlu, Ö., and M. Alay**. 2019. "Anti-Drone sistemleri." *STM Teknolojik Düşünce Merkezi.* https://thinktech.stm.com.tr/uploads/docs/1608997770_stm-anti-drone-savunma-sistemleri.pdf.

**Şafak, Yeni.** 2016. *PKK askeri birliğe bombalı drone ile saldıracaktı.* https://www.yenisafak.com/gundem/pkk-askeri-birlige-bombali-drone-ile-saldiracakti-2546484.

**Şen, Ş.** 2018. "PKK'dan DEAŞ'ın drone taktiği." *Yeni Şafak.* https://www.yenisafak.com/dunya/pkkdan-deasin-drone-taktigi-3408887.

**Takvim.** 2020. *MSB: PKK'nın drone ile düzenlediği saldırı engellendi.* https://www.takvim.com.tr/guncel/2020/08/20/son-dakika-haberi-msb-pkknin-drone-ile-duzenledigi-saldiri-engellendi.

**The Economist.** 2019. Drone attacks cut Saudi Arabia's oil output byhalf. https://www.economist.com/middle-east-and-africa/2019/09/15/drone-attacks-cut-saudi-arabias-oil-output-by-half.

**Timokhin, A.** 2019. "Türkiye uses laser weapon technology to shoot down Chinese UAV Wing Loong II in Libya." *Army Recognition.*

**TR Military News.** 2020. *Aselsan İHASAVAR'ların teslimatları son sürat devam ediyor.* https://www.trmilitarynews.com/aselsan-ihasavarlarin-teslimatlari-son-surat-devam-ediyor/.

**TRT Haber.** 2021. *Batman'da askeri tesise 3 maket uçak ile saldırı girişimi.* https://www.trthaber.com/haber/turkiye/batmanda-askeri-tesise-3-maket-ucak-ile-saldiri-girisimi-582218.html.

**___.** 2023. *Drone'ların korkulu rüyası ILTER ihracat başarılarına yenisini ekledi.* https://www.trthaber.com/haber/savunma/dronlarin-korkulu-ruyasi-ilter-ihracat-basarilarina-yenisini-ekledi-796675.html.

**Ulusal Savunm.** 2024a. *KALKA erken uyarı hava savunma sistemleri.* https://ulusalsavunma.com.tr/kalka-erken-uyari-hava-savunma-sistemleri/.

___. 2024b. *Ürünler: yönlendirilmiş drone-savarlar.* https://ulusalsavunma.com.tr/ihamix/.

**Yeni Şafak.** 2019. *PKK askeri kışlaya maket uçakla saldırdı.* https://www.yenisafak.com/gundem/pkk-askeri-kislaya-maket-ucakla-saldirdi-3448394.

**Yıldırım, G.** 2017. "Yerli drone silahı avrupa yolunda." *Anadolu Ajansı.* https://www.aa.com.tr/tr/turkiye/yerli-drone-silahi-avrupa-yolunda-/875317.

___. 2020. "Drone Tehdidine Karşı İlter Kalkanı." *Anadolu Ajansı.* https://www.aa.com.tr/tr/bilim-teknoloji/drone-tehdidine-karsi-ilter-kalkani/2020464.

**Zmysłowski, D., P. Skokowski, and J. M. Kelner.** 2023. "Anti-drone Sensors, Effectors, and Systems – A Concise Overview." *The International Journal on Marine Navigation and Safety of Sea Transportation* 17 (2): 455-461. doi:10.12716/1001.17.02.23.

**Zwijnenburg, W.** 2023. "Between terror strikes and targeted killings: the evolving role of drone warfare in Iraq." *PAX.* https://paxforpeace.nl/wp-content/uploads/sites/2/2023/10/PAX_Between-Terror-Strikes-and-Targeting-Killings.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Detection of Buried Landmines using a Convolutional Autoencoder trained on Simulated prompt Gamma Spectra

**Konstantinos KARAFASOULIS, PhD***

*Laboratory Teaching Staff, Hellenic Army Academy, Athens, Greece
e-mail: ckaraf@gmail.com

## Abstract

The detection of buried landmines remains a persistent challenge in security and humanitarian demining. In this work, we present an indirect detection methodology based on the analysis of prompt gamma-ray emissions induced by 14 MeV neutron irradiation. A high-resolution $LaBr_3$ detector captures the gamma spectra arising from neutron interactions with soil constituents and buried explosives. A Convolutional Neural Network (CNN) autoencoder, trained in an unsupervised manner, models the intrinsic spectral response of soil under varying moisture conditions. Anomalies between reconstructed and measured spectra are used to infer the presence of subsurface anomalies consistent with landmines. Monte Carlo simulations, conducted with the Geant4 toolkit, generate a comprehensive dataset encompassing a soil matrix under various moisture levels. The proposed system demonstrates sensitivity to buried antipersonnel landmines at shallow depths, validating the integration of neutron activation analysis and deep learning for advanced landmine detection applications.

**Keywords:**
Landmine Detection; Artificial Intelligence; Autoencoders; Anomaly Detection; Neutron Activation; Gamma Radiation.

**Article info**
Received: 12 May 2025; Revised: 6 June 2025; Accepted: 10 June 2025; Available online: 27 June 2025

Citation: Karafasoulis, K. 2025. "Detection of Buried Landmines using a Convolutional Autoencoder trained on Simulated prompt Gamma Spectra." *Bulletin of "Carol I" National Defence University*, 14(2): 114-127. https://doi.org/10.53477/2284-9378-25-19

The global impact of landmines, particularly anti-personnel and anti-tank devices, continues to be a significant humanitarian and security concern. According to (Landmine and Cluster Munition Monitor 2024), at least 58 countries remain affected by these hidden threats, which cause thousands of casualties annually, the majority of whom are civilians. Beyond the tragic human cost, landmines pose long-term socio-economic barriers by rendering agricultural lands unusable, displacing populations, and impeding post-conflict recovery. From a military standpoint, effective detection and clearance of landmines are also of strategic importance, as they directly affect troop mobility, operational planning, and the safety of personnel in both combat and peacekeeping missions. Consequently, advancing landmine detection technologies serves both humanitarian objectives and tactical military needs, reinforcing global stability and mission success in affected regions.

Conventional landmine detection technologies include metal detectors, ground-penetrating radar (GPR), and trained detection animals (e.g., dogs or rats). While these methods have proven utility, each comes with critical limitations. Metal detectors suffer from high false-positive rates due to metallic clutter in post-conflict zones, while GPR performance can be significantly degraded by soil heterogeneity or high moisture content. Biological detection methods, although accurate, are resource-intensive and difficult to deploy at scale.

To overcome these limitations, nuclear-based techniques, particularly those exploiting neutron interrogation, offer unique advantages. One such technique is Prompt Gamma Neutron Activation Analysis (PGNAA), which relies on bombarding the ground with fast neutrons (e.g., 14 MeV) and detecting the resulting prompt gamma rays emitted when the neutrons interact with various nuclei in the soil and hidden objects. PGNAA enables non-destructive elemental analysis, particularly effective in detecting nitrogen, a key component of many explosive compounds such as TNT, RDX, and PETN.

Gamma-ray lines commonly associated with explosive materials include:

- 10.8 MeV (from the reaction $^{14}N(n,\gamma)^{15}N$)
- 2.22 MeV (from $^{1}H(n,\gamma)^{2}H$)
- 6.13 MeV (from $^{16}O(n,n'\gamma)^{16}O$)

The presence of these characteristic gamma lines can indicate anomalies beneath the surface. However, interpreting this spectral information is not trivial. Gamma spectra are influenced by numerous environmental variables, including soil composition, moisture content, density, and the presence of innocuous materials (e.g., plastic waste, buried vegetation). These confounding factors can lead to false positives when using rule-based or threshold-based detection approaches.

To address this complexity, we propose a machine learning-based solution utilising a Convolutional Neural Network (CNN) autoencoder. A CNN autoencoder is a type

of neural network trained to compress and reconstruct its input—in this case, the full gamma spectrum recorded by a $LaBr_3$ detector. During training, the autoencoder learns to represent the "normal" variability of gamma spectra from soil-only conditions, without requiring examples containing landmines. This unsupervised learning paradigm provides several strategic benefits:

- **No need for explosive training data:** Since acquiring real spectra from buried landmines is dangerous, scarce, and often ethically restricted, training exclusively on simulated or measured background soil spectra removes this dependency.
- **Anomaly detection capability:** Once trained, the autoencoder can identify deviations from the learned spectral patterns. When a spectrum from soil containing a buried landmine is input, it cannot be reconstructed accurately, resulting in a high reconstruction error, which flags it as anomalous.
- **Low false positive sensitivity:** Because the model captures the complex spectral variability of legitimate background conditions, it is less prone to overreacting to harmless but structurally different materials that might affect threshold-based systems.

In this paper, we present a simulation-driven study using Geant4 to generate prompt gamma spectra for one soil type at varying moisture levels (0%, 10%, and 20%). A CNN autoencoder is trained solely on these background spectra and evaluated against test cases containing an anti-personnel landmine buried at 5 cm and 10 cm depths. The spectra span 2048 bins up to 15 MeV, reflecting high-resolution detection capabilities. This approach enables robust anomaly detection, even in diverse and noisy soil environments, with high potential for real-world deployment in both humanitarian demining and military applications.

## Related Work

Landmine detection has long been a multidisciplinary challenge, combining geophysics, nuclear physics, and increasingly, artificial intelligence. Classical methods such as metal detectors, ground-penetrating radar (GPR), and infrared imaging are widely used but struggle with specific limitations: metal detectors generate high false-positive rates in cluttered environments, GPR sensitivity drops in heterogeneous or moist soil, and infrared sensors are easily confounded by surface conditions.

As a result, neutron-based techniques have emerged as highly promising alternatives due to their ability to probe elemental composition rather than just physical or metallic properties. Among these, Prompt Gamma Neutron Activation Analysis (PGNAA) and Neutron Backscattering (NBT) have received considerable attention. PGNAA, in particular, utilises fast neutrons (e.g., 14 MeV) to induce prompt gamma-ray emissions that reveal elemental signatures, such as those from nitrogen, a common marker for high explosives.

Experimental and simulation studies have validated the effectiveness of nuclear-based systems for detecting explosives. For example, (Elsheikh 2018) modelled a thermal neutron-induced gamma-ray sensor to detect prompt gamma emissions from $^{14}N(n,\gamma)^{15}N$ reactions, capturing the key 10.8 MeV gamma line. Similarly, (Viesti, et al. 2006) demonstrated the use of neutron backscattering techniques for humanitarian demining, emphasising the importance of minimising soil moisture to enhance detection contrast. Additional experimental validation was carried out by specialists (Clifford, et al. 2007) who fielded a thermal neutron activation system for military confirmation of buried anti-tank mines, confirming effectiveness up to 30 cm depths under various environmental conditions.

However, nuclear techniques come with their own challenges, particularly interpreting the complex gamma-ray spectra produced during interrogation. Spectra are affected not only by the elemental composition of the explosive but also by the surrounding soil type, density, and humidity. These environmental confounders can induce misleading spectral features and elevate false alarm rates when traditional thresholding or peak-matching methods are used.

To overcome these limitations, machine learning approaches have been introduced (Xue, et al. 2022). They compared multiple supervised learning models, including fully connected neural networks (FCNN), LightGBM, and radial basis function networks (RBF), to classify PGNAA spectra from different explosive burial conditions. They reported over 96% classification accuracy even under high soil moisture conditions using full-spectrum inputs, underscoring the potential of data-driven models over hand-engineered feature extraction.

Yet, supervised methods inherently depend on labelled training data, often requiring spectra containing real landmines or explosive materials—data that is difficult to obtain due to ethical, safety, and logistical constraints. To mitigate this, unsupervised models, particularly autoencoders, offer a robust alternative. Autoencoders are neural networks that learn to reproduce their input data; deviations between input and output (reconstruction error) can be used to detect anomalies. When trained solely on background spectra (e.g., soil without explosives), any significant deviation caused by the presence of a landmine will manifest as a high reconstruction error.

Other studies, such as those by (Datema, et al. 2003) proposed novel imaging approaches using neutron backscattering and Monte Carlo simulations with GEANT4 to localise hydrogen anomalies in the topsoil. These approaches laid the groundwork for simulation-driven training data, critical for training unsupervised models in the absence of real explosive data.

In this paper, we propose a novel landmine detection framework that combines PGNAA spectral interrogation with a convolutional autoencoder trained solely on simulated background spectra. By learning the underlying structure of gamma-

ray spectra from soil without explosives, the model detects anomalies based on reconstruction error when exposed to spectra influenced by buried explosives. This unsupervised approach addresses the dual challenges of limited access to real explosive data and complex spectral variability caused by environmental factors. Leveraging convolutional layers, the autoencoder effectively captures localised spectral features, such as gamma peaks and Compton edges, enabling robust detection of nitrogen-rich explosives while maintaining adaptability across diverse field conditions.

## Methodology

### *1.1. Experimental Setup for PGNAA Simulation*

The simulation environment for this study replicates a realistic PGNAA (Prompt Gamma Neutron Activation Analysis) system using a 14 MeV fast neutron source placed within a protective and moderating assembly designed to optimise gamma-ray yield while reducing background noise.

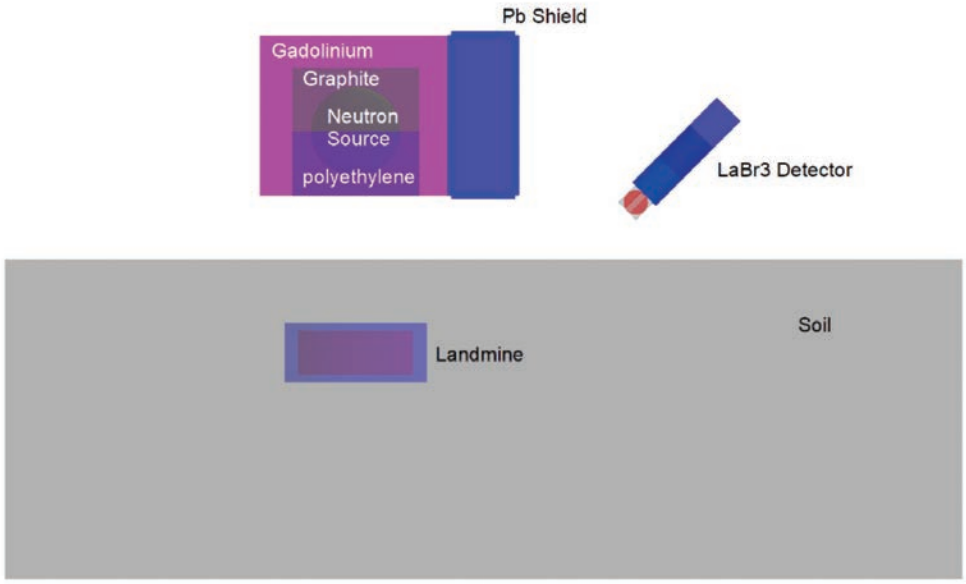



**Figure 1** Schematic of the simulation geometry. The neutron source is located at the centre of a hollow spherical shell enclosed in a gadolinium-lined box (open at the bottom). The upper hemisphere of the shell is graphite for neutron reflection, while the lower hemisphere is polyethylene for neutron moderation. The assembly is suspended 10 cm above the soil surface. A lead shield is positioned between the source and the $LaBr_3$ detector to suppress unwanted gamma flux. Simulations include buried mines at 5 cm or 10 cm depth within a 150 cm × 160 cm × 50 cm soil volume.

The neutron source is placed at the centre of a hollow spherical shell with a radius of 7 cm, housed within a gadolinium-lined box measuring 30 cm × 30 cm × 25 cm, open at the bottom. The spherical shell surrounding the source is divided into two hemispheres: the upper half is composed of graphite, serving as a neutron reflector to direct neutrons downward toward the soil, while the lower half is made of polyethylene, acting as a moderator to thermalise fast neutrons.

This configuration enhances the likelihood of neutron interactions within the target medium. The entire assembly is positioned 10 cm above the ground surface. For

simulations involving buried mines, the mine is located at a depth of 5 cm or 10 cm within a soil volume measuring 150 cm × 160 cm × 50 cm (depth). The detailed geometry of the mine is presented in Table 3. In control simulations without the mine, the same soil setup is used to evaluate the background response.

A lead (Pb) shield is placed to the right of the source, between the source and the $LaBr_3$ detector, to attenuate scattered and prompt gamma rays from unwanted directions. This shielding improves signal clarity and reduces detector saturation. The detector is located 50 cm away from the source at an inclination angle of 45°, providing an optimised detection geometry for capturing prompt gamma emissions resulting from neutron interactions in the soil.

### *1.2. Gamma Spectrum Dataset Generation*

All gamma-ray spectra used in this study were generated using the Geant4 Monte Carlo simulation toolkit (Agostinelli, et al. 2003). The target region in the simulation consists of one soil type, simulated under three distinct moisture conditions: 0%, 10%, and 20% by weight. Soil compositions, elemental content, and density parameters are detailed in Table 1.

**TABLE NO. 1**
**Soil Composition**

| **Humidity** | 0% | 10% | 20% |
|---|---|---|---|
| **Density ($g/cm^3$)** | 1.47 | 1.63 | 1.84 |
| **Elements** | **Mass Fraction** | | |
| Na | 0.008 | 0.007 | 0.007 |
| H | 0.000 | 0.011 | 0.022 |
| K | 0.022 | 0.019 | 0.017 |
| Mg | 0.032 | 0.029 | 0.026 |
| Ca | 0.037 | 0.034 | 0.051 |
| Fe | 0.064 | 0.058 | 0.030 |
| Al | 0.071 | 0.064 | 0.057 |
| Si | 0.296 | 0.267 | 0.237 |
| O | 0.470 | 0.511 | 0.553 |

To ensure a statistically robust gamma emission profile, a total of 750,000 gamma-ray interaction events in the detector were recorded, resulting from neutron interactions with soil at three different moisture levels: dry, 10%, and 20% moisture. Specifically, 250,000 gamma-ray events were collected for each soil condition following neutron-induced reactions. The deposited energy spectra on the $LaBr_3$ detector were then

processed to reflect the detector's intrinsic energy resolution by applying Gaussian smearing to the recorded gamma energies, using a full width at half maximum (FWHM) defined as:

$$FWHM = A\sqrt{\frac{E}{E_c}} \quad (1)$$

where A = 19.2 keV and $E_c$ = 662 keV. This smearing procedure accurately reflects the energy resolution characteristics of the $LaBr_3$ detector, thereby enhancing the realism of the simulated spectra.

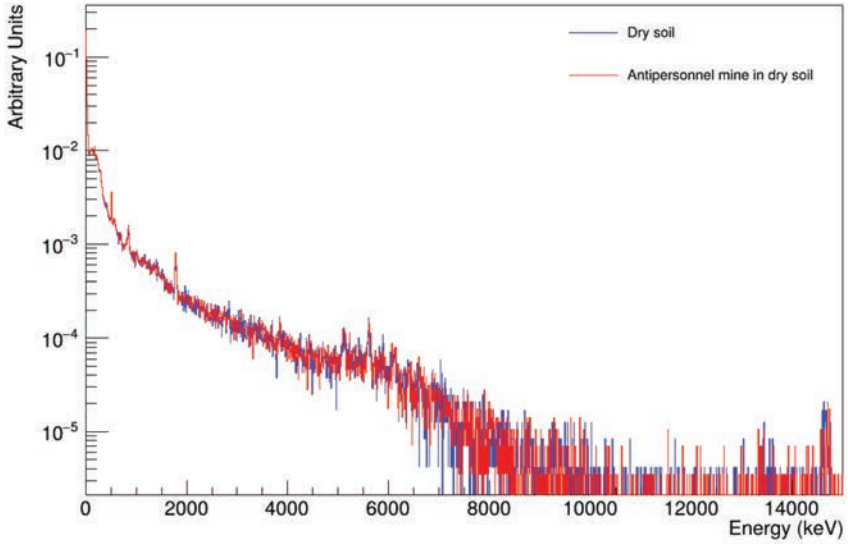



**Figure 2** Comparison of gamma-ray spectra following neutron activation. The blue line represents the spectrum of dry soil alone, while the orange line corresponds to dry soil containing a buried antipersonnel landmine at a depth of 5 cm. The presence of the landmine induces characteristic spectral features, distinguishing it from the background soil response.

Subsequently, 10,000 gamma spectra were generated per soil composition from the smeared interaction dataset. Each spectrum was constructed by randomly sampling the simulated events, promoting statistical diversity and improving dataset robustness. These spectra consisted of 2,048 discrete energy bins, spanning the full dynamic range of the $LaBr_3$ detector (0–15 MeV), with each spectrum normalised to a total of 50,000 events. Representative gamma spectra for dry soil and the landmine model buried in dry soil at 5cm depth are presented in Figure 2.

### *1.3. CNN Autoencoder Architecture*

To model the background spectral distribution and perform anomaly detection, a 1D Convolutional Neural Network (CNN) autoencoder (Adari and Alla 2024) was implemented using Keras (Gulli and Pal 2017). The architecture was designed to progressively compress high-dimensional spectral data and reconstruct it from a learned latent representation, allowing for anomaly detection via reconstruction error.

**TABLE NO. 2**
**CNN Autoencoder Architecture**

| Layer Type | Filters | Nodes | Kernel Size | Stride | Activation | Padding |
|---|---|---|---|---|---|---|
| 1D Input | - | 2048 | - | - | - | - |
| **Encoder** | | | | | | |
| Conv1D | 32 | - | 3 | 1 | ReLU | Same |
| Max Pooling 1D | - | - | 2 | 2 | - | Same |
| Conv1D | 64 | - | 3 | 1 | ReLU | Same |
| Max Pooling 1D | - | - | 2 | 2 | - | Same |
| Conv1D | 128 | - | 3 | 1 | ReLU | Same |
| Max Pooling 1D | - | - | 2 | 2 | - | Same |
| **Decoder** | | | | | | |
| Upsampling 1D | - | - | - | 2 | - | - |
| Conv1D | 128 | - | 3 | 1 | ReLU | Same |
| Upsampling 1D | - | - | - | 2 | - | - |
| Conv1D | 64 | - | 3 | 1 | ReLU | Same |
| Upsampling 1D | - | - | - | 2 | - | - |
| Conv1D | 32 | - | 3 | 1 | ReLU | Same |
| Conv1D | 1 | - | 3 | 1 | Sigmoid | Same |
| 1D Output | - | 2048 | - | - | - | - |

The encoder consists of three convolutional layers with filter sizes of 32, 64, and 128, each using a kernel size of 3, a stride of 1, and 'same' padding. Each convolutional layer is followed by a MaxPooling layer with a pool size of 2 and a stride of 2, which progressively reduces the spatial resolution of the input spectrum while increasing feature depth.

The decoder mirrors the encoder's structure in reverse. It begins with the most compressed latent feature map and reconstructs the full-resolution spectrum using three convolutional layers in reverse order (128 → 64 → 32 filters), interleaved with Upsampling layers to restore the original dimensionality. The final output layer uses a Sigmoid activation function to reproduce the 2048-bin normalised spectrum.
The complete architecture, including kernel parameters and feature map dimensions at each stage, is presented in Table 2.

### *1.4. Training Procedure*

The CNN autoencoder was implemented and trained using the Adam optimiser (Kingma and Ba 2015) with default parameters and a Mean Squared Error (MSE) loss function:

$$\text{MSE} = \frac{1}{2048}\sum_{i=1}^{2048}(y_i - \hat{y}_i)^2 \quad (2)$$

where $y_i$ is the true count in bin $i$ of the real spectrum and $\hat{y}_i$ is the predicted count in bin $i$ by the autoencoder.

The model was trained for 5 epochs using a batch size of 128 spectra. The training dataset, as described in Section 1.2, comprises spectra obtained from three different soil types: dry, 10% moisture, and 20% moisture. To ensure robust model evaluation, 70% of this dataset was used for training and the remaining 30% for validation. The training and validation MSE per batch iteration is shown in Figure 3, which confirms the absence of overfitting. The training curve exhibits a smooth convergence, and the validation loss closely tracks the training loss throughout the epochs.

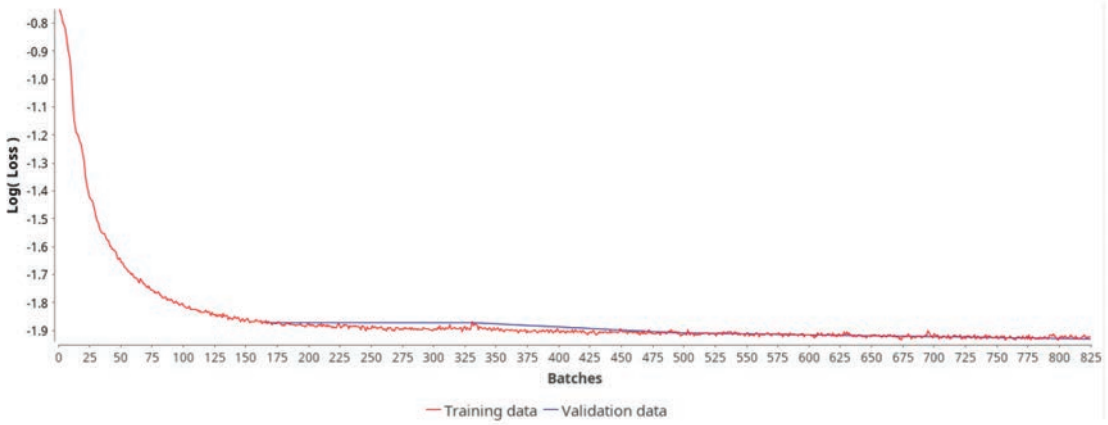



**Figure 3** Logarithm of the mean squared error (MSE) per batch during training of the CNN autoencoder. The red curve represents the training samples, while the blue curve corresponds to the validation samples. The close agreement between the two curves indicates stable learning, with no signs of overtraining observed.

Since the model was only trained on spectra representing clean soil, the learned representation reflects the natural variability of soil-only gamma emissions, allowing the system to detect anomalies (i.e., landmine presence) during evaluation.

## Model Evaluation

To assess the performance of the CNN autoencoder in detecting buried landmines, we conducted a dedicated set of simulations involving a realistically modelled anti-personnel landmine filled with TNT (trinitrotoluene) (Table no. 3). The simulated explosive object was buried in the dry soil used during training, under identical physical and radiological conditions, thereby ensuring consistent experimental parameters between training and evaluation.

The geometry and chemical composition of the landmine were modelled based on standard anti-personnel ordnance specifications. The explosive material, TNT, was represented using its molecular composition ($C_7H_5N_3O_6$), emphasising the high nitrogen content, which serves as a key elemental indicator in PGNAA-based detection methods. The mine casing was assumed to be made of plastic, consistent with real-world low-metal mines.

**TABLE NO. 3**
**CNN Antipersonnel Mine Specifications**

| | |
|---|---|
| **Material** | $C_7H_5N_3O_6$), |
| **Mass (kg)** | 2.939 |
| **Density (g/cm$^3$)** | 1.65 |
| **Shape** | Cylindrical |
| **Radius (cm)** | 7.0 |
| **Height (cm)** | 7.0 |
| **Case Material** | Low-Density Plastic |
| **Case Width (cm)** | 2.1 |

Two burial depths were examined to reflect practical detection thresholds in both humanitarian and military demining operations.

- 5 cm below the soil surface (shallow burial)
- 10 cm below the soil surface (moderate depth)

Using the same PGNAA system configuration described previously — including the graphite reflector, polyethylene moderator, gadolinium box, and lead shielding — we simulated neutron interactions with soil containing the buried landmine.
For each burial depth (5 cm and 10 cm), a total of 300,000 gamma-ray interaction events in the detector were recorded, resulting from neutron interactions with the buried landmine simulated using Geant4. From these events, 10,000 gamma-ray spectra were randomly sampled per depth, with each spectrum consisting of 2,048 energy bins spanning up to 15 MeV. This procedure mirrors the methodology employed for generating the background soil spectra and ensures consistent statistical representation across all evaluation conditions.

Each of the 10,000 landmine-influenced gamma spectra was processed through the trained CNN autoencoder, which had been trained solely on soil-only gamma spectra. To rigorously evaluate the model's anomaly detection capability, the test set also included 30,000 additional soil-only spectra, comprising 10,000 samples each for dry soil, 10% moisture, and 20% moisture conditions, that were entirely distinct from the training set. Since the autoencoder had not encountered either landmine-contaminated spectra or these specific soil-only spectra during training, its reconstruction was guided exclusively by its learned representation of typical, unperturbed soil spectra. This setup allowed the model to highlight discrepancies in the landmine spectra as potential anomalies.

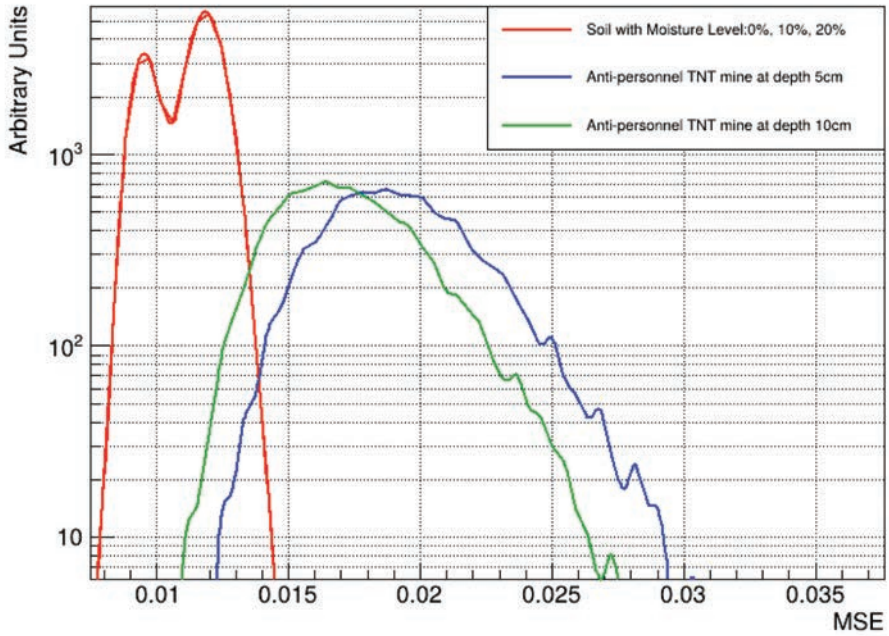



**Figure 4** MSE distributions for clean soil spectra (all humidity levels combined) and landmine-buried spectra at 5 cm and 10 cm depths. Clean soil samples show low reconstruction errors, while landmine-affected spectra produce significantly higher MSE values. The clear separation between distributions demonstrates the autoencoder's ability to detect anomalies and supports its use for identifying buried landmines using PGNAA.

The Mean Squared Error (MSE) between each input spectrum and its reconstructed output was used as the reconstruction error, serving as a direct metric for spectral anomaly detection. Spectra corresponding to clean soil samples consistently yielded low MSE values, reflecting high-fidelity reconstructions by the autoencoder. In contrast, spectra from soil containing a buried TNT landmine produced significantly higher MSE values due to the presence of spectral features unfamiliar to the model. Figure 4 illustrates the distribution of reconstruction errors across all test conditions, including the aggregated MSE distribution for clean soil spectra under all three moisture levels (0%, 10%, and 20%), as well as for landmine-influenced spectra at burial depths of 5 cm and 10 cm. A clear statistical separation is evident between the background and anomalous spectra, confirming the model's sensitivity to landmine-induced gamma signatures.

A detection threshold was defined at a reconstruction error of 0.01445, above which an input spectrum is classified as anomalous. This threshold yielded a signal detection efficiency of 97.46% for landmines buried at 5 cm and 87.31% for those at 10 cm. These values reflect the fraction of landmine spectra correctly identified as anomalies while maintaining robust separation from the background soil distributions. The performance drop at 10 cm burial depth can be attributed to the greater attenuation of both neutrons and gamma rays, which reduces the prominence of spectral deviations introduced by the explosive material.

Nevertheless, even at 10 cm depth, the anomaly signal remains distinctly detectable relative to the background, demonstrating the system's potential applicability to a range of buried threat scenarios. These results validate the effectiveness of the CNN autoencoder in detecting subsurface explosives based on prompt gamma spectral anomalies and further support the method's scalability for detecting larger, more easily detectable anti-tank mines in practical field conditions.

## Discussion

The results of this study affirm the viability of using a convolutional autoencoder trained solely on simulated prompt gamma spectra from soil to detect anomalies indicative of buried antipersonnel landmines. A critical component of this framework is the $LaBr_3$ detector's ability to resolve high-energy gamma lines, notably the emission from nitrogen—a primary elemental marker in common explosives such as TNT and RDX. To enable this, the detector was simulated with a maximum energy range of 15 MeV, necessitating precise electronic design in practical implementations. Achieving reliable performance at such high energies requires low-noise analog front-end circuitry, high-speed digitisers with extended dynamic range, and probably temperature-compensated calibration systems to ensure energy linearity and resolution. Sensitivity analyses revealed that constraining the detection range, for example by lowering the upper energy limit to 12 MeV to reduce hardware complexity or shielding requirements, results in a measurable decline in detection performance. This is attributed to the attenuation or loss of critical high-energy gamma lines that provide discriminatory power between background soil and explosive-containing spectra.

Despite this, the model still maintains its anomaly detection capability, although with a narrower margin of separation between landmine and background samples in the reconstruction error space. Importantly, while the present evaluation focused on antipersonnel landmines, which are compact, low-metal content devices and thus represent a challenging detection scenario, the methodology is expected to yield even more robust results when applied to larger anti-tank mines. These devices typically contain greater quantities of explosive material and present larger target volumes for neutron interrogation, resulting in stronger gamma-ray signals and higher anomaly contrast. Consequently, the approach outlined here offers a scalable foundation for landmine detection systems, balancing detection sensitivity, spectral resolution, and practical engineering constraints in future experimental or field deployments.

## Conclusions

This study presents a novel, simulation-driven approach for detecting buried anti-personnel landmines using prompt gamma spectra generated by 14 MeV neutron interrogation and analysed through a convolutional autoencoder trained exclusively on soil-only spectra. The model successfully identified landmine-induced spectral

anomalies across varying soil moisture conditions, without requiring training on explosive data. A detection threshold of 0.01445 in reconstruction error enabled signal detection efficiencies of 97.46% and 87.31% for landmines buried at 5 cm and 10 cm depths, respectively. These results highlight the effectiveness of integrating high-resolution gamma detection with unsupervised deep learning for anomaly detection. Future efforts will focus on expanding the dataset to encompass more diverse soil types and explosive materials, enhancing robustness to environmental noise, and evaluating the method's performance on anti-tank mines and smaller ordnance, with the goal of developing a scalable and field-deployable landmine detection system.

## References

**Adari, S., and S. Alla.** 2024. *Beginning Anomaly Detection Using Python-Based Deep.* Berkeley: Apress.

**Agostinelli, S, Allison J., Amako K., Apostolakis J., Araujo H., Arce P., Asai M., et al.** 2003. "Geant4—a simulation toolkit." *Nuclear Instruments and Methods A* 506 (3): 250-303. doi:10.1016/S0168-9002(03)01368-8.

**Clifford, E.T.H., J.E. McFee, H. Ing, H.R. Andrews, D. Tennant, E. Harper, and A.A. Faust.** 2007. "A militarily fielded thermal neutron activation sensor for landmine detection." *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 579 (1): 418-425. doi:10.1016/j.nima.2007.04.091.

**Datema, C.P., V.R. Bom, and C.W.E. van Eijk.** 2003. "Monte Carlo simulations of landmine detection using neutron backscattering imaging." *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment* 513 (1-2): 398-402.

**Elsheikh, N.A.A.** 2018. "Monte Carlo modelling of a neutron-induced gamma-ray sensor for landmine or explosive detection." *Journal of Radiation Research and Applied Sciences* 11 (4): 403–407. https://doi.org/10.1016/j.jrras.2018.08.004.

**Gulli, A., and S. Pal.** 2017. *Deep learning with Keras.* Packt Publishing Ltd.

**Kingma, Diederik P, and Jimmy Ba.** 2015. "Adam: A Method for Stochastic Optimization." *arXiv preprint.* doi:10.48550/arXiv.1412.6980.

**Landmine and Cluster Munition Monitor.** 2024. "Landmine Monitor 2024." https://www.the-monitor.org/reports/landmine-monitor-2024.

**Nebbia, Ginacarlo and Juergen Gerl.** 2005. "Detection of buried landmines and hidden explosives using neutron, X-ray and gamma-ray probes." *Europhysics News* 36: 119-123. doi:10.1051/epn:2005403.

**Viesti, G., M. Lunardon, G. Nebbia, M. Barbui, M. Cinausero, G. D'Erasmo, M. Palomba, A. Pantaleo, J. Obhođaš, and V. Valković.** 2006. "The detection of landmines by neutron backscattering: Exploring the limits of the technique." *Applied Radiation and Isotopes* 64 (6): 706-716. doi:10.1016/j.apradiso.2005.12.017.

**Xue, Hui, Guang-Yu Shi, De-Dong He, and Si-Yuan Chen.** 2022. "Simulation Study on Landmines Detection by Pulsed Fast Thermal Neutron Analysis." *Arabian Journal for Science and Engineering* 47 (1): 879-885. doi:10.1007/s13369-021-05742-0.

**Funding Information**
This research received no external funding.

**Conflict of Interest**
The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**Data Availability**
The data that support the findings of this study are openly available in the Open Science Framework at https://osf.io/udwqp/

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Shariah Law and Religious Rights in a Multi-religious Society: examining its Introduction for Muslims in Western Nigeria

**Mahmud A. OSHO, PhD***

*Department of Political Science and Public Administration, Faculty of Humanities and Social Sciences, Al-Hikmah University, Adewole, Ilorin, Kwara State
e-mail: maosho@alhikmah.edu.ng

## Abstract

The introduction of Shariah law in Western Nigeria is primarily aimed at protecting the religious rights of Muslims, ensuring their ability to practice Islamic legal principles within a secular framework. This study explores the socio-political implications of Shariah in a multi-religious society, emphasizing that its application is exclusively for Muslims and does not infringe on the rights of non-Muslims. The research examines the historical evolution of Shariah in Nigeria, the constitutional provisions for religious freedom, and the legal pluralism that allows for multiple judicial systems to coexist. While the adoption of Shariah law strengthens the identity and religious autonomy of Muslims, it also raises concerns about political interpretations and interfaith relations. Using qualitative methods, including case studies and a questionnaire, the study assesses how Shariah law functions within a diverse society, ensuring that it remains a voluntary legal system for Muslims. The findings highlight the importance of upholding religious rights while maintaining national unity and peaceful coexistence. The study concludes with recommendations for policy frameworks that balance religious freedom, legal inclusivity, and social harmony in Western Nigeria.

**Keywords:**
Shariah Law; Religious Rights; Western Nigeria; Legal Pluralism; Peaceful Coexistence.

**Article info**
Received: 14 April 2025; Revised: 12 May 2025; Accepted: 16 May 2025; Available online: 27 June 2025

Citation: Osho, M.A. 2025. "Shariah Law and Religious Rights in a Multi-religious Society: examining its Introduction for Muslims in Western Nigeria" *Bulletin of "Carol I" National Defence University*, 14(2): 128-153. https://doi.org/10.53477/2284-9378-25-20

The introduction of Shariah law in Western Nigeria, particularly since the early 2000s, has generated substantial socio-political debate. Although Shariah has been a longstanding component of the legal system in Northern Nigeria, its gradual adoption and recognition in parts of the Western region, especially in states with significant Muslim populations such as Osun, Oyo, and Lagos, marks a notable development in Nigeria's religious and legal landscape.

This shift has raised questions about the potential security implications of Shariah law's adoption in a historically multi-religious and politically diverse region. Specifically, there is a concern that the socio-political effects could evolve into a security problem, particularly for non-Muslim communities, secular activists, and political actors who perceive the move as a step towards religious domination. The fear is that it may lead to sectarian polarization, erosion of trust in state institutions, and violent confrontations, especially if perceived as unde rmining Nigeria's secular constitution.

The broader discourse is often framed within the narrative of Islamization, wherein the legal recognition of Shariah is seen by some as a strategy to impose Islamic norms on a pluralistic society. This narrative has fueled inter-religious suspicion and political rivalry, making the matter not only a legal or religious issue but a potential threat to social cohesion and national security.

Nevertheless, advocates for Shariah law in Western Nigeria argue that its adoption is constitutionally legitimate and confined to personal and civil matters involving Muslims alone. They highlight that Nigeria practices legal pluralism, recognizing customary and religious laws alongside secular statutes. In this view, the implementation of Shariah law does not contravene the Nigerian Constitution but enhances the right of Muslims to live in accordance with their religious beliefs.

This study critically assesses the social and political ramifications of Shariah law's emergence in Western Nigeria. It evaluates its implications for religious rights, interfaith harmony, and the stability of democratic governance, while also interrogating the fears surrounding national unity and the perceived erosion of secularism. Through this analysis, the study aims to clarify whether the Shariah system promotes peaceful coexistence or inadvertently lays the groundwork for sectarian division and conflict.

## Research Objectives

The primary objective of this study is to examine the socio-political implications of the introduction of Shariah law in Western Nigeria, particularly in the context of a multi-religious society. Specifically, the study aims to:

1. Analyze the rationale behind the introduction of Shariah law in Western Nigeria and its role in protecting the religious rights of Muslims.
2. Examine the constitutional and legal framework that supports the coexistence of Shariah law within Nigeria's secular legal system.
3. Investigate public perceptions and reactions to the introduction of Shariah law, particularly in relation to concerns about the Islamization of Nigeria.
4. Assess the impact of Shariah law on interfaith relations, governance, and social cohesion in Western Nigeria.
5. Provide policy recommendations for ensuring religious harmony, legal pluralism, and peaceful coexistence in the region.

## Scope of the Study

This study focuses on the socio-political implications of the introduction of Shariah law in Western Nigeria, particularly in the context of a multi-religious society. The research examines the historical background, legal framework, and contemporary debates surrounding the implementation of Shariah law in the region. While Shariah has been practiced in Northern Nigeria for decades, its recent introduction in parts of Western Nigeria has generated discussions on religious rights, legal pluralism, and national unity.

The study is limited to Western Nigeria, covering selected states where discussions or efforts toward implementing Shariah law have gained attention. It investigates the perspectives of various stakeholders, including religious scholars, legal practitioners, policymakers, and members of both Muslim and non-Muslim communities. The study does not focus on the theological intricacies of Islamic jurisprudence, but rather on the socio-political dimensions of its application.

Furthermore, the research assesses the constitutional provisions that permit the coexistence of multiple legal systems in Nigeria and how Shariah law operates within this framework. The study also explores public perceptions, addressing concerns about whether its introduction signals an attempt at Islamization or simply the exercise of religious rights by Muslims. The findings will contribute to policy recommendations aimed at promoting peaceful coexistence, legal inclusivity, and religious tolerance in Nigeria.

## Literature Review

The implementation of Shariah law in Nigeria has been a subject of scholarly discourse, particularly regarding its socio-political implications in a multi-religious society. While much of the existing literature focuses on Shariah law in Northern Nigeria, the introduction of Islamic legal principles in Western Nigeria has sparked

debates on religious rights, legal pluralism, and national unity. This literature review explores historical perspectives on Shariah in Nigeria, its constitutional basis, its socio-political implications, and public perceptions surrounding its introduction in Western Nigeria.

***Historical Background of Shariah Law in Nigeria***

Shariah law has deep historical roots in Nigeria, dating back to the pre-colonial era when Islamic legal systems governed many parts of the northern region. According to Uthman (2019), Islamic jurisprudence was introduced in present-day Nigeria through trade, migration, and Islamic scholars who played a key role in shaping governance structures in various emirates. The Sokoto Caliphate, established in the 19th century, institutionalized Shariah law, making it the dominant legal system in Northern Nigeria (Last 1967).

With the advent of British colonial rule, Shariah law was significantly restricted, and the introduction of a common law system led to its relegation primarily to matters of personal status, such as marriage, inheritance, and family law (Ostien 2007). However, the reintroduction of full Shariah law in some northern states in 1999 reignited debates on its role within Nigeria's pluralistic legal system. This historical background is crucial in understanding contemporary discussions about its extension to Western Nigeria.

***Constitutional and Legal Framework for Shariah Law in Nigeria***

Nigeria operates a legal system that accommodates three major sources of law: statutory law, customary law, and Islamic law. The 1999 Constitution of the Federal Republic of Nigeria recognizes Shariah law as part of the country's legal framework, particularly in the adjudication of personal matters for Muslims (Constitution of Nigeria 1999, Section 277). However, scholars such as Nwauche (2010) argue that while Shariah law is constitutionally recognized, its extension beyond personal matters remains a contentious issue in multi-religious regions.

The constitution guarantees freedom of religion under Section 38, allowing individuals and religious groups to practice their faith freely. This provision serves as the legal basis for the introduction of Shariah law in Western Nigeria, as proponents argue that it merely provides Muslims with the option to resolve personal and civil disputes through Islamic legal principles. However, critics warn that such developments could create legal fragmentation, leading to conflicts over jurisdiction between Shariah and secular courts (Ezeilo 2011).

***Socio-Political Implications of Shariah Law in Western Nigeria***

The introduction of Shariah law in Western Nigeria has raised significant socio-political concerns, particularly regarding interfaith relations and national cohesion. According to Abikan (2013), Shariah law is designed to serve only Muslims and does

not interfere with the rights of non-Muslims. However, some scholars argue that its implementation could deepen religious divisions in an already polarized society. Ojo (2016) contends that the fear of Islamization is largely driven by misinformation and political rhetoric rather than the actual practice of Shariah law.

One major concern is the potential impact on governance and political processes. Scholars such as Falola (2018) suggest that the introduction of Shariah law in Western Nigeria could influence electoral politics, as religious identity may become a more significant factor in political alignments. Additionally, it could affect interfaith relations, as non-Muslims may perceive the move as an attempt to expand Islamic influence beyond its traditional strongholds. However, empirical studies indicate that where Shariah is properly implemented, it has contributed to social order and justice within Muslim communities (Peters 2003).

***Public Perceptions and Debates on Shariah in Western Nigeria***

Public reactions to the introduction of Shariah law in Western Nigeria have been mixed. While many Muslims welcome the initiative as a means of upholding their religious rights, others, particularly non-Muslims, view it with suspicion. According to a survey conducted by Yusuf (2021), 65% of Muslims in Western Nigeria support Shariah law for personal and civil matters, while 30% of non-Muslims express concerns about its broader implications for the region's secular legal framework.

Religious leaders and civil society organizations have played a crucial role in shaping public discourse on the issue. While Islamic scholars emphasize that Shariah law is a voluntary system meant only for Muslims, some Christian organizations argue that it could create a precedent for religious legal systems that may later extend to non-Muslims (Adegbite 2020). Despite these concerns, legal experts highlight that Shariah law remains an optional legal system, and its introduction in Western Nigeria aligns with constitutional provisions on religious freedom (Ostien 2007).

The reviewed literature highlights the complex legal, historical, and socio-political dimensions of Shariah law in Nigeria. While its introduction in Western Nigeria is intended to protect the religious rights of Muslims, it has also sparked debates on national unity, legal pluralism, and interfaith relations. Existing studies emphasize the need for clear legal frameworks, public awareness, and interfaith dialogue to ensure that Shariah law functions as an inclusive and non-divisive legal system. While previous studies have focused on the legal debates surrounding Shariah, few have empirically assessed public opinion in Western Nigeria regarding its implementation. This study addresses that gap through a questionnaire designed to capture diverse views on the socio-political and legal implications of Shariah law. Further empirical research is needed to assess its long-term impact on governance and social cohesion in Western Nigeria.

## Theoretical Framework

The introduction of Shariah law in Western Nigeria can be analyzed through various theoretical lenses that explain the interplay between law, religion, and society in a multi-religious state. This study adopts the Legal Pluralism Theory, Social Contract Theory, and Religious Rights Theory to provide a comprehensive understanding of the socio-political implications of Shariah law in Western Nigeria. These theories help explain the coexistence of multiple legal systems, the protection of religious freedoms, and the balance between religious autonomy and national unity.

***Legal Pluralism Theory***

Legal pluralism is a theoretical framework that recognizes the existence of multiple legal systems within a single political entity. According to Griffiths (1986), legal pluralism exists when two or more legal systems operate simultaneously within a given society. Nigeria, as a multi-religious and multi-ethnic state, exhibits legal pluralism by allowing statutory law, customary law, and Islamic law to function alongside one another.

The introduction of Shariah law in Western Nigeria fits within this theoretical framework, as it reflects the constitutional recognition of multiple legal traditions. Legal scholars such as Merry (1988) argue that legal pluralism allows for the accommodation of diverse cultural and religious identities, ensuring that different communities have access to justice systems that align with their values. In Nigeria, Section 277 of the 1999 Constitution permits the establishment of Shariah courts for Muslims, reinforcing the idea that legal pluralism is a constitutional reality rather than an attempt to impose a singular legal structure.

However, critics argue that legal pluralism can lead to legal fragmentation, jurisdictional conflicts, and tensions between religious and secular legal principles (Benda-Beckmann 2002). While Shariah law is intended only for Muslims, concerns about its implications for governance, social cohesion, and interfaith relations must be addressed within the broader context of Nigeria's legal pluralism.

***Social Contract Theory***

The Social Contract Theory, as developed by scholars such as Hobbes (1651), Locke (1689), and Rousseau (1762), provides a framework for understanding the balance between individual freedoms and state authority. This theory posits that individuals consent to be governed by a political and legal system in exchange for the protection of their rights and freedoms.

In the context of Nigeria, the introduction of Shariah law for Muslims can be seen as an extension of the social contract, where Muslims exercise their constitutional rights to religious freedom and legal self-determination. According to Rawls (1971), a just society must accommodate the diverse interests of its citizens while ensuring

fairness and equality under the law. By allowing Muslims to resolve personal and civil matters through Shariah law, the Nigerian legal system upholds the principle of religious freedom without necessarily infringing on the rights of non-Muslims.

However, the application of Social Contract Theory also raises questions about national unity and equal citizenship. If different legal systems apply to different religious groups, some scholars argue that it could lead to social divisions and legal inequalities (Kymlicka 1995). Thus, while the introduction of Shariah law is consistent with the social contract principle of religious autonomy, it also requires careful management to ensure it does not undermine national cohesion.

***Religious Rights Theory***

Religious Rights Theory focuses on the protection of individuals' rights to practice their religion freely within a legal and political framework. This theory is rooted in international human rights instruments such as Article 18 of the Universal Declaration of Human Rights (United Nations 1948) and Article 8 of the African Charter on Human and Peoples' Rights (Organization of African Unity 1981), both of which recognize freedom of religion as a fundamental human right.

Nigeria's constitutional framework aligns with this theory by guaranteeing religious freedom under Section 38 of the 1999 Constitution, which allows individuals to practice and propagate their religion without interference. The introduction of Shariah law in Western Nigeria is, therefore, justified under this theory as a means of protecting the religious rights of Muslims, ensuring that they have access to a legal system that aligns with their faith.

According to An-Na'im (2008), religious rights must be understood within the broader context of human rights and legal pluralism. He argues that the implementation of religious laws, such as Shariah, should not be seen as a violation of secular principles but rather as an affirmation of the right to religious self-determination. However, he also cautions that religious legal systems must be implemented in a way that ensures they do not infringe on the rights of others or create divisions within society.

The theoretical frameworks of Legal Pluralism, Social Contract, and Religious Rights provide a multidimensional understanding of the introduction of Shariah law in Western Nigeria. Legal Pluralism explains how multiple legal systems coexist within the Nigerian legal framework. Social Contract Theory highlights the balance between religious autonomy and national unity, while Religious Rights Theory underscores the constitutional and human rights basis for the application of Shariah law. These theories collectively demonstrate that while Shariah law serves as a means of protecting Muslim religious rights, its implementation must be managed carefully to maintain national cohesion and interfaith harmony.

## Methodology

This study adopts a primarily quantitative research approach, supported by qualitative contextual insights, to examine the socio-political implications of Shariah law in Western Nigeria. The focus is on understanding how the implementation of Shariah affects religious rights, interfaith relations, and legal pluralism. The methodology section outlines the research design, population, sample, sampling techniques, data collection instruments, and methods of analysis. The research is structured to provide empirical evidence grounded in primary data, complemented by legal and doctrinal analysis to ensure a robust interpretation of the findings.

***Research Design***

The study employs a dominant quantitative design, using a structured questionnaire to collect measurable data on public perceptions and experiences related to the introduction of Shariah law in Western Nigeria. This is complemented by qualitative content analysis of legal and policy documents, which serves primarily to provide contextual background and frame the empirical results within relevant constitutional and political discourses.

Unlike earlier versions of the study that placed more emphasis on qualitative methods, this revised design prioritizes the use of structured questionnaires to generate statistically analyzable data. This approach allows for clearer differentiation among respondent categories and provides a basis for cross-tabulation using variables such as religious affiliation, professional status, income level, and educational background.

***Population of the Study***

The study targets five key sub-groups within the Western Nigerian context:

- Legal experts (scholars and practitioners familiar with Islamic and constitutional law)
- Religious leaders (Muslim and Christian clerics)
- Policymakers (government officials in legal and judicial sectors)
- Political scientists and academic analysts
- General residents, drawn from religiously and ethnically diverse communities in states where debates about Shariah law have gained traction (e.g., Lagos, Oyo, Osun)

The selection of this population is based on their relevance to the legal, religious, and civic discourse surrounding Shariah law. Unlike a general population survey, this study strategically engages those with direct stakes or informed perspectives on the issue, while still incorporating a broad spectrum of public opinion through lay respondents.

***Sampling Technique and Sample Size***

To achieve a representative and analytically useful dataset, the study employs a multi-stage sampling strategy:

- Purposive sampling was used to select legal experts, policymakers, and religious leaders based on their roles and expertise.
- Stratified random sampling was applied to select general respondents, ensuring proportional representation across key demographic categories (religion, gender, socio-economic status, and location).

A total of 300 respondents participated in the study, distributed as follows:

- 50 legal experts
- 50 religious leaders
- 50 government officials and policymakers
- 150 members of the general public

This stratification allowed the researcher to perform comparative analysis across different occupational and social strata. Future analysis includes exploring differences in perception based on income levels, professional status, and religious affiliation, which are key variables captured in the survey instrument.

***Rationale for Instrument Selection***

Although interviews—especially with religious leaders and legal scholars—would provide richer narrative insight, the decision to use a structured questionnaire was based on three considerations:

1. Comparability and scalability: Questionnaires allow for the aggregation of responses from a relatively large and diverse sample, enabling generalizations about trends and public attitudes.
2. Time and resource constraints: Given the geographic scope and diversity of the target population, administering interviews at scale would have been less feasible.
3. Quantitative analysis priority: The study's emphasis on measuring and comparing perceptions across demographic categories necessitates a standardized data collection tool.

That being said, insights drawn from legal documents, official statements, and academic commentary have been employed to contextualize the statistical data, forming the qualitative background to the study.

***Data Collection Methods***

*1. Primary Data*

- Structured Questionnaire: Administered both in print and digitally, the questionnaire contained closed-ended questions using a Likert scale to assess attitudes toward Shariah law, perceptions of religious marginalization, and support for legal pluralism. It also included demographic items (religion, profession, income bracket, education) for subgroup analysis.

*2. Secondary Data*

- Legal and Constitutional Documents: Including the 1999 Constitution of the Federal Republic of Nigeria, relevant Shariah court rulings, and international

human rights instruments.

- Academic Literature: Scholarly texts and journal articles on legal pluralism, Islamic law, and Nigerian federalism.
- Media Sources and Policy Reports: Statements by religious leaders, government responses, and civil society commentaries.

***Data Analysis Techniques***

*Quantitative Data Analysis*

- Descriptive statistics (frequencies, percentages, bar charts, pie charts) are used to illustrate the overall distribution of responses.
- Cross-tabulations and comparative analysis are employed to explore relationships between variables such as profession, income level, and support for Shariah law.

*Qualitative Data Analysis*

- Content analysis of legal and policy texts was conducted to understand the constitutional legitimacy, political framing, and interfaith concerns surrounding Shariah law.
- Rather than serving as a stand-alone qualitative study, these findings serve to complement and enrich the interpretation of survey data.

***Ethical Considerations***

- Informed Consent: Participants were briefed on the objectives of the study and signed informed consent forms.
- Anonymity and Confidentiality: All responses were anonymized; data were stored securely.
- Objectivity and Neutrality: The researcher maintained neutrality and refrained from influencing responses or leading participants.

By focusing primarily on quantitative primary data and embedding qualitative insights in supporting roles, this study responds to critical feedback by offering a more empirical and comparative account of the socio-political effects of Shariah law in Western Nigeria. The decision to structure the study in this manner enhances both the validity and policy relevance of the findings.

## Questionnaire Data Presentation and Analysis

This section presents and analyzes the data collected from respondents on the topic "Shariah Law and Religious Rights in a Multi-Religious Society: Examining Its Introduction for Muslims in Western Nigeria." The total number of respondents was 300. The data were collected using structured questionnaires and analyzed quantitatively.

## 1. Demographic Profile of Respondents

### Age Distribution:

The majority of the respondents fall within the age bracket of 31–45 years (39.67%), followed by those aged 18–30 years (29.33%). About 24.33% are between 46–60 years, while a small percentage are above 60 years (4.00%) or below 18 years (2.67%).

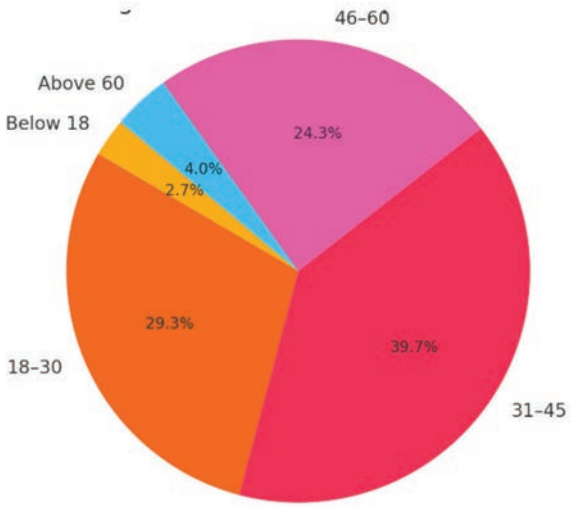



**Figure 1** Age Distribution of Respondents

### Gender:

A significant portion of the respondents were male (70.33%), while females constituted 29.67%. This gender distribution reflects broader male participation in religious and legal discourse within the studied population.

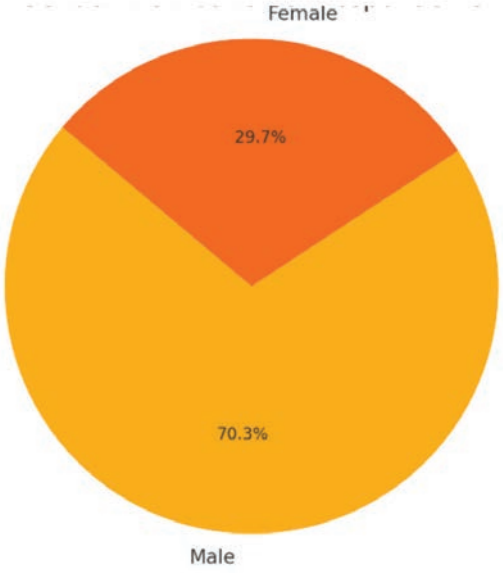



**Figure 2** Gender Distribution of Respondents

**Religious Affiliation:**
The respondents are predominantly Muslims (85.67%), with Christians accounting for 14.33%. This skewed distribution is consistent with the focus of the study on Muslim perspectives.

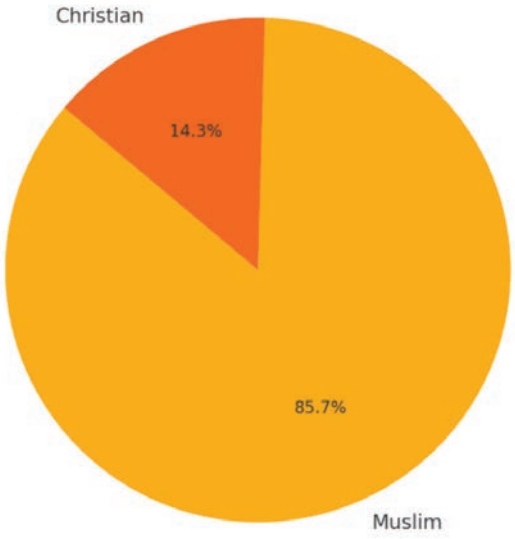



**Figure 3** Religious Affiliation of Respondents

**2. Respondents' Knowledge and Perceptions of Shariah Law**

**Understanding of Shariah Law:**
An overwhelming majority (89.67%) affirmed they have a basic understanding of Shariah law, indicating that most participants are informed on the subject matter.

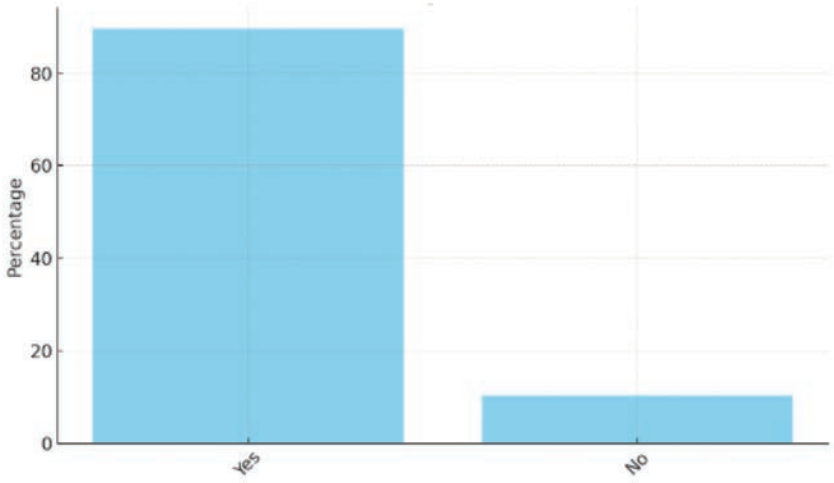



**Figure 4** Understanding of Shariah Law

**Necessity of Shariah Law in Western Nigeria:**
71.67% of respondents believe that Shariah law is necessary in Western Nigeria. Meanwhile, 23.33% disagreed, and 5% remained undecided. This shows strong support among Muslims for the institutionalization of Shariah in the region.

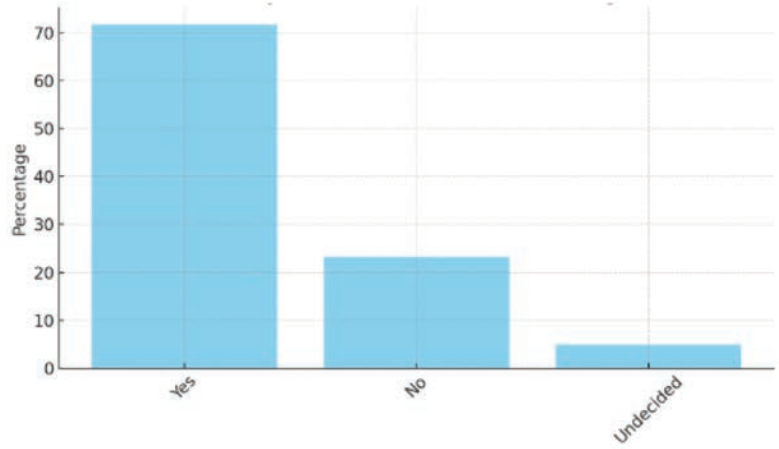



**Figure 5** Necessity of Shariah Law in Western Nigeria

**Applicability of Shariah Law:**
Most respondents (71.33%) believe that Shariah law should apply only to Muslims, with 16% suggesting it can apply to both Muslims and non-Muslims, and 12.67% arguing it should apply to all Nigerian citizens. This reflects the perception that Shariah law is a religious legal system meant for adherents of Islam.

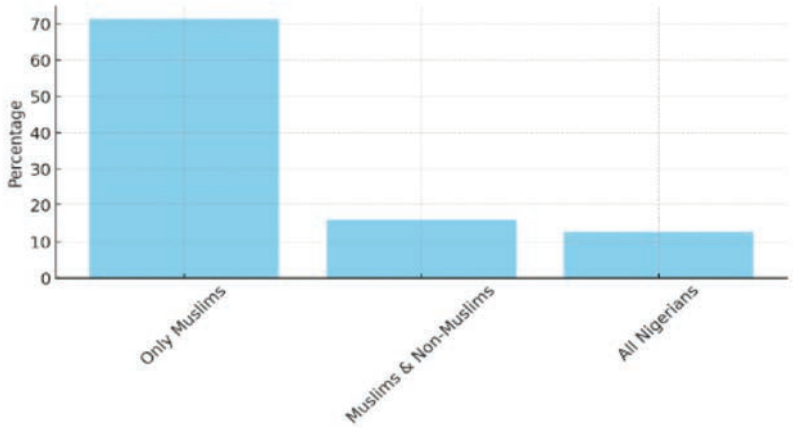



**Figure 6** Applicability of Shariah Law

**3. Perceived Impacts of Shariah Law**

**Promotion of Religious Harmony:**
66.33% believe that the introduction of Shariah law in Western Nigeria will promote religious harmony. However, 23% disagreed, and 10.67% were unsure. The majority view reflects confidence in Shariah law as a tool for peace among its proponents.

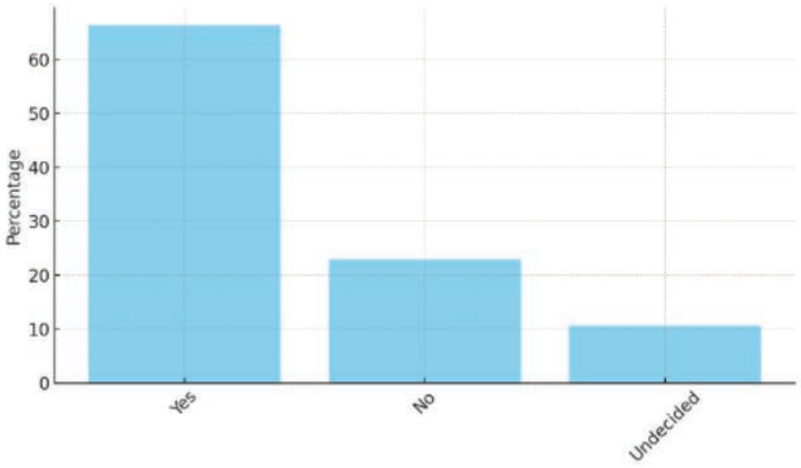



**Figure 7** Shariah Promote Religious Harmony?

**Shariah Law as a Tool for Islamization:**
When asked whether Shariah law is a tool for Islamizing Nigeria, 43.67% strongly disagreed and 21.67% disagreed. However, 17.67% agreed, and 10% strongly agreed, with 7% choosing a neutral stance. This indicates that while a majority reject the claim, a considerable minority entertain suspicions of political motives behind its introduction.

The findings reveal a strong awareness and favorable perception of Shariah law among Muslims in Western Nigeria. The data suggest that a significant portion of the Muslim population views Shariah law not only as a religious necessity but also as a mechanism for promoting moral discipline and social order. However, concerns about the broader implications for national unity and religious harmony persist, especially among non-Muslim minorities.

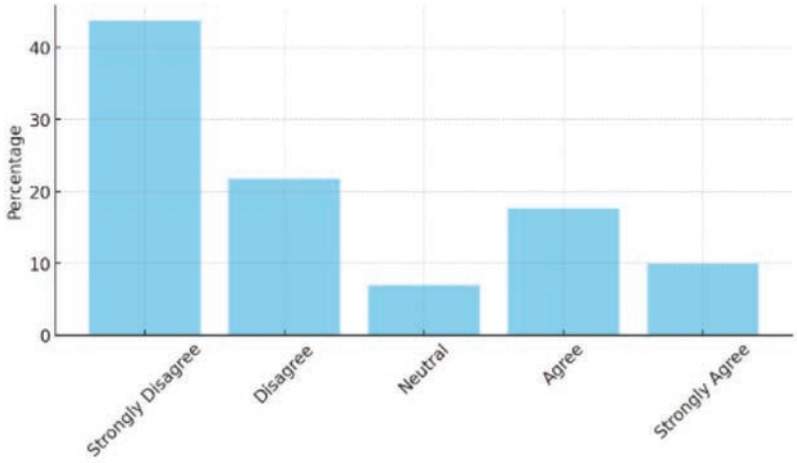



**Figure 8** Is Shariah a Tool for Islamization?

## 4. Legal and Human Rights Considerations

**Constitutional Support:**
According to the respondents, 60.87% believe the Nigerian Constitution supports the implementation of Shariah law in Western Nigeria. However, 24.64% were unsure, and 14.49% explicitly stated that the Constitution does not support it. This divergence highlights the need for clearer legal interpretation and education on constitutional provisions relating to religious law.

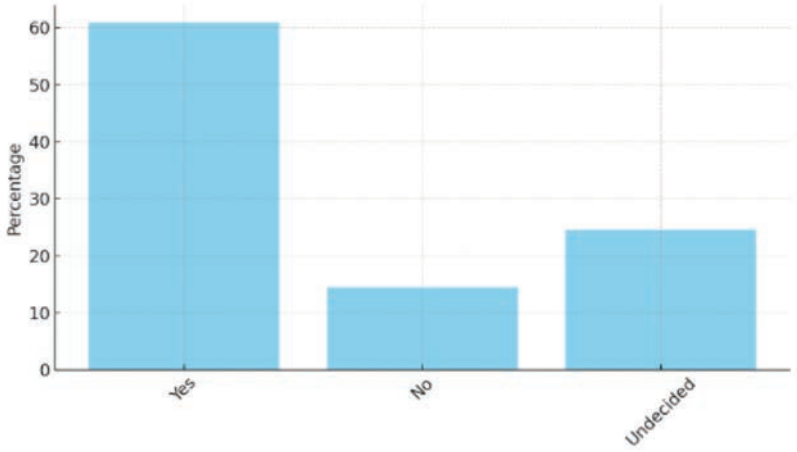



**Figure 9** Constitutional Support for Shariah Law

**Alignment with International Human Rights Standards:**
A similar pattern emerged with regard to human rights. 59.42% of respondents believe Shariah law aligns with international human rights standards, while 21.74% disagreed and 18.84% were unsure. While the majority accept compatibility, a sizable minority express concerns that warrant further engagement and legal clarification.

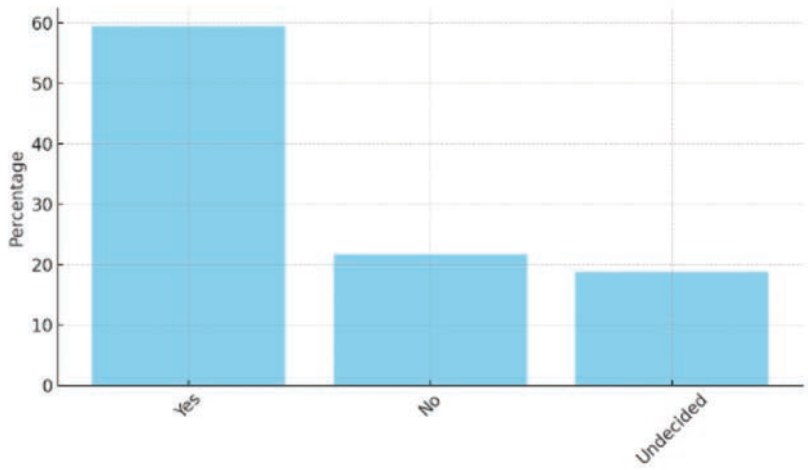



**Figure 10** Shariah Law & International Human Rights

**Protection of Non-Muslim Rights:**
Respondents suggested several strategies to ensure that the rights of non-Muslims are not infringed upon. These include:

- "*By defining its application in the law and proper enforcement.*"
- "*Muslims in public service to act honourably.*"
- "*By going through appropriate channels.*"

These perspectives underline the importance of ethical governance, legal safeguards, and responsible implementation.

**Suggested Reforms:**
To balance religious rights and national unity, participants recommended reforms such as:

- "*Education and enlightenment.*"
- "*Recognition of Shariah panels and establishment of Shariah Courts of Appeal.*"
- "*National orientation agencies should sensitize the public.*"

These focus on civic education, institutional reform, and national sensitization to foster religious inclusivity.

**Peaceful Coexistence:**
Recommendations for promoting peaceful coexistence between Muslims and non-Muslims included:

- "*Promote religious harmony.*"
- "*Encourage mutual understanding.*"
- "*Continue interfaith education.*"

This reflects a shared desire for mutual respect and sustained dialogue in a pluralistic society.

**Additional Insights:**
Some respondents raised critical reflections, with comments such as:

- "*No need for the implementation in Western Nigeria.*"
- "*Training of Arabic and Islamic teachers in Western Nigeria.*"

These reflect both skepticism and constructive suggestions for inclusive religious education.

Overall, while support for Shariah law remains strong among respondents, the data indicates a thoughtful awareness of the legal and human rights implications. There is also a proactive call for frameworks that uphold both religious and civic values within a democratic setting.

**The Rationale Behind the Introduction of Shariah Law in Western Nigeria and Its Role in Protecting the Religious Rights of Muslims**
Nigeria's legal system accommodates customary, statutory, and Islamic laws. While Shariah law is well-established in the North, its growing relevance in Western

Nigeria—a religiously diverse region—merits analysis. This essay explores the rationale behind its introduction and its role in protecting Muslim religious rights within Nigeria's constitutional and socio-religious context.

***Historical and Religious Rationale***

Shariah predates colonialism in Nigeria, particularly in the North and parts of the Yoruba West like Ilorin (Na'Allah 2009). Colonial rule introduced English law but did not completely displace Islamic personal law. Post-1999 democratic reforms revived Muslim demands for Shariah, viewed not just as law but a comprehensive way of life based on the Qur'an and Sunnah (Oba 2002). Its reintroduction supports religious identity amid increasing secularism.

***Constitutional and Legal Justification***

Though Nigeria's 1999 Constitution is secular, it guarantees freedom of religion (Section 38) and allows states to establish Shariah Courts of Appeal (Sections 275–279) (FRN 1999). Shariah in Western Nigeria is voluntary and limited to Muslims, reflecting legal pluralism and protecting the rights of all citizens (Ostien 2007).

***Cultural Identity and Religious Rights***

Shariah law helps preserve Muslim cultural and religious identity by governing personal matters like marriage, inheritance, and custody (Lenta 2005). It ensures Muslims can resolve such issues in line with their faith, aligning with the constitutional guarantee of religious freedom (Eze 1984).

***Democratic Expression and Legal Pluralism***

Advocacy for Shariah has emerged through democratic channels, showing it is both a religious and political demand for legal inclusion (Ostien 2007). Nigeria's legal pluralism—statutory, customary, and Islamic—supports Shariah's legitimacy in the West (Oba 2011).

***Challenges and Caution***

Despite its benefits, Shariah's expansion can raise concerns about inter-religious conflict and politicization (Yadudu 2000). To avoid this, its application must remain voluntary and focused on personal matters, respecting Nigeria's religious diversity.

The introduction of Shariah in Western Nigeria stems from historical, religious, constitutional, and cultural imperatives. It affirms Muslims' right to practice their faith within Nigeria's plural legal framework. However, careful and inclusive implementation is essential to maintain religious harmony and uphold constitutional principles.

**The Constitutional and Legal Framework Supporting the Coexistence of Shariah Law within Nigeria's Secular Legal System**

Nigeria operates a plural legal system, accommodating customary, Islamic (Shariah), and statutory laws within a single framework. Though constitutionally secular,

Nigeria also recognizes the religious and cultural diversity of its people. This has enabled Shariah law to function alongside secular law, particularly in civil matters involving Muslims. This essay outlines the constitutional and legal basis for Shariah's coexistence within Nigeria's secular structure.

***Secularism and Religious Freedom***

Section 10 of the 1999 Constitution states that no government in Nigeria shall adopt a state religion (FRN 1999). Despite this, Section 38 guarantees freedom of thought, conscience, and religion, including the right to manifest and propagate one's faith. This balance allows religious laws like Shariah to exist within a secular legal framework.

***Recognition of Shariah Law***

Sections 275–279 permit states to establish Shariah Courts of Appeal with jurisdiction limited to civil matters involving Muslims—such as marriage, inheritance, and guardianship. These courts operate only with the voluntary consent of Muslim parties and do not affect non-Muslims, thereby upholding religious pluralism and legal coexistence.

***Legal Pluralism and Customary Law***

Alongside Shariah law, customary law is also recognized and applied in personal and communal matters. Like Shariah, customary courts are limited in scope and must comply with constitutional standards (Oba 2002). This reflects Nigeria's pragmatic embrace of legal pluralism, respecting cultural diversity within a unified legal order.

***Judicial Precedents***

The judiciary has upheld the constitutionality of Shariah law where it applies only to Muslims and does not violate federal law or the rights of others. In Kano State Government v. Federation (Supreme Court of Nigeria 2006), the Supreme Court confirmed the legitimacy of Shariah courts in civil cases involving Muslims, provided non-Muslims are not affected.

***Checks and Human Rights Protections***

Chapter IV of the Constitution guarantees fundamental rights such as fair hearing (Section 36), equality (Section 42), and protection from discrimination. Any perceived infringement under Shariah law can be challenged in the regular courts, including the Court of Appeal and the Supreme Court.

***Federalism and State Autonomy***

Nigeria's federal structure allows states to establish courts and legal systems responsive to local needs. States like Kwara, Oyo, and Kano have used this autonomy to implement Shariah courts for Muslim communities. However, these efforts must conform to the national constitution and respect federal laws.

The coexistence of Shariah law with Nigeria's secular legal system reflects the country's commitment to legal pluralism, federalism, and religious freedom. The Constitution enables Shariah law in civil matters among Muslims while protecting the rights of all citizens. This balance sustains unity in diversity and ensures that religious laws function within constitutional boundaries.

**Public Perceptions and Reactions to the Introduction of Shariah Law in Nigeria: Concerns About Islamization**

The reintroduction of Shariah law in several northern Nigerian states since 1999 has generated considerable debate and concern, particularly relating to the perceived Islamization of Nigeria. While proponents view it as a legitimate legal framework for Muslim personal and civil matters, critics—especially from southern and non-Muslim populations—have expressed apprehension about its implications for national unity, secularism, and human rights.

Shariah law was officially adopted in twelve northern states of Nigeria, starting with Zamfara State in 1999, under the leadership of Governor Ahmad Sani Yerima. This development followed the return to democratic governance and was portrayed as a move to enhance moral standards and justice for Muslims (Paden 2005). Supporters of Shariah law argue that it aligns with the religious identity and aspirations of the Muslim-majority northern population and operates within the constitutional provision for freedom of religion and legal pluralism (Ostien 2007). They contend that Shariah courts only have jurisdiction over civil and personal matters involving consenting Muslims, and therefore do not violate the rights of non-Muslims.

However, this legal development provoked strong reactions from various quarters. Many Christians and secular-minded Nigerians saw the adoption of Shariah law as a step toward the Islamization of Nigeria, a constitutionally secular state (Ibrahim 2004). These fears were fueled by reports of harsh punishments such as amputation and stoning, and concerns that such practices were incompatible with international human rights standards and Nigeria's constitution. The Christian Association of Nigeria (CAN), human rights organizations, and some southern politicians criticized the move, warning that it could deepen religious divisions and threaten national cohesion (Marshall 2002).

Furthermore, non-Muslims residing in Shariah-implementing states often felt marginalized, especially in cases where the application of certain moral codes, such as bans on alcohol or gender segregation in public transportation, affected the general population (Yusuf 2013). Even among Muslims, reactions were mixed. Some questioned the political motives behind the sudden reimplementation of Shariah, suspecting it was being used to gain political legitimacy or distract from economic and governance challenges (Kendhammer 2013).

Despite these controversies, federal authorities in Nigeria have largely allowed the implementation of Shariah to proceed, provided it does not infringe on constitutional

rights or extend beyond its prescribed jurisdiction. The Nigerian judiciary, in notable decisions, such as *Kano State Government v. Federation* (Supreme Court of Nigeria 2006), upheld the legality of Shariah civil jurisdiction for Muslims, reinforcing the principle of legal pluralism under Nigeria's constitution.

In conclusion, the introduction of Shariah law in northern Nigeria continues to elicit polarized responses, shaped by religious, political, and regional identities. While many Muslims see it as an expression of religious freedom and moral justice, others fear it signals a gradual erosion of secularism and inclusivity. These conflicting perceptions underscore the complex interplay between law, religion, and identity in Nigeria's pluralistic society, and they highlight the ongoing need for dialogue, legal clarity, and sensitivity to Nigeria's diverse population.

**The Impact of Shariah Law on Interfaith Relations, Governance, and Social Cohesion in Western Nigeria**

Western Nigeria, predominantly Yoruba, is noted for religious pluralism and interfaith harmony. While Shariah law is not fully implemented in the region as in Northern Nigeria, its advocacy by Muslim communities has sparked debate over its implications for interfaith relations, governance, and social cohesion.

***Interfaith Relations***

Shariah discourse has sometimes strained interfaith ties. Christian groups, notably the Christian Association of Nigeria (CAN), fear marginalization and the erosion of Nigeria's secular character (Marshall 2002). Conversely, Muslim advocates see the denial of Shariah courts as religious discrimination, especially since Christian ecclesiastical courts are recognized (Yusuf 2013). Despite these tensions, the Yoruba tradition of religious tolerance helps maintain peace.

***Governance and Legal Pluralism***

Western states like Lagos and Osun have avoided full Shariah implementation but accommodate aspects of Islamic law through customary courts in matters such as marriage and inheritance. Full implementation would require constitutional reforms and may provoke political resistance (Kendhammer 2013). As a result, governance in the region emphasizes caution, balance, and inclusivity.

***Social Cohesion and Identity***

Yoruba society's deep-rooted religious tolerance allows space for limited Shariah application among Muslims without undermining social harmony. For Muslims, Shariah represents an ethical and moral framework rather than a political tool. Its application in civil matters—on a voluntary basis—can coexist with Nigeria's secular legal system, in line with constitutional guarantees (FRN 1999, Sections 38 and 275). Experiences from Northern states like Zamfara and Kano show that Shariah, with proper safeguards and inclusive dialogue, can promote justice and social order. In Western Nigeria, where Muslims are a significant demographic in states like Osun,

Oyo, Ogun, and Lagos, calls for limited Shariah reflect a legitimate demand for religious self-determination (Ostien 2007).
Rather than fragmenting society, legal pluralism can affirm identity and dignity across religious lines. Paden (2005) emphasizes that Nigeria's strength lies in managing, not erasing, its diversity.

The Shariah discourse in Western Nigeria highlights the need to balance religious freedom with social cohesion. With transparency, dialogue, and legal safeguards, Shariah can operate peacefully within Nigeria's secular framework. The goal should be justice for all—through respect, equity, and inclusion.

**Contextual and Comparative Analysis: Shariah Law in Northern and Western Nigeria**

Understanding the impact of Shariah law in Western Nigeria requires a comparison with Northern Nigeria, where its implementation is more entrenched. Both regions have sizable Muslim populations, but historical, legal, and societal contexts shape differing outcomes for governance, religious rights, and national unity.

***Shariah Law in Northern Nigeria***

Shariah has deep roots in Northern Nigeria, dating back to pre-colonial Islamic emirates and persisting through colonial and post-colonial periods (Loimeier 2012). Its reintroduction as state law began in 1999 with Zamfara and spread to 12 other northern states. There, Shariah covers civil and criminal matters and is administered through specialized courts (Ostien 2007).

Key features include:

- Institutionalization: Shariah courts fully integrated into the judicial system.
- Broad Jurisdiction: Includes criminal, civil, commercial, and family law.
- Popular Support: Minimal resistance due to religious homogeneity (Paden 2005).

However, concerns persist about human rights, gender equity, and constitutional compatibility (Ibrahim and Igbuzor 2002).

***Shariah Law in Western Nigeria***

In contrast, states like Lagos, Oyo, and Osun operate within a plural legal culture of customary, Islamic, and statutory law (Olaniyan 2020). Shariah applies only to civil matters among Muslims and lacks criminal jurisdiction.

Key characteristics include:

- Voluntary Use: Muslims may opt into Shariah courts for personal law.
- Restricted Scope: No authority over criminal cases, avoiding constitutional conflict (Ostien 2007).
- Religious Sensitivity: Given the religious diversity, its expansion is often contested (Falola 2009).

Shariah's discussion in the West has sparked fears of Islamization, political division, and communal tension (Adebanwi 2004).

***Similarities and Differences***

Commonalities include:

- Constitutional Legitimacy: Section 38 supports freedom of religion.
- Muslim-Specific Jurisdiction: Shariah applies only to Muslims (Nmehielle 2004).
- Political Symbolism: Used for identity and political mobilization.

Differences lie in institutional reach and social reception: Shariah is state law in the North, while in the West, it remains a civil legal option amid interfaith sensitivities.

***Socio-Political Implications***

In the North, Shariah is woven into the legal and religious system, albeit with some challenges. In the West, its implementation is more controversial, raising fears of marginalization and threatening secular principles. These tensions highlight the need for careful, region-specific approaches to legal pluralism, interfaith harmony, and national unity.

**Policy Recommendations for Religious Harmony, Legal Pluralism, and Peaceful Coexistence in Western Nigeria**

***1. Strengthen Constitutional Guarantees and Legal Frameworks***

- Affirm Religious Freedom: Reinforce constitutional protections under Section 38 (freedom of thought, conscience, and religion) to ensure that individuals can practice their faith without fear of discrimination or coercion.
- Recognize Legal Pluralism: Institutionalize mechanisms that recognize and respect the coexistence of statutory, customary, and religious legal systems—especially in matters of personal law (e.g., marriage, inheritance, and family law).
- Safeguard Minority Rights: Ensure that Shariah or any other religious laws are implemented only for adherents of that faith, with clear legal boundaries protecting non-adherents from undue influence or imposition.

***2. Promote Inclusive Governance and Representation***

- Interfaith Advisory Councils: Establish state-level and local government interfaith advisory councils composed of leaders from Islamic, Christian, and traditional communities to deliberate on policies, mediate conflicts, and build consensus on sensitive issues.
- Diverse Representation in Public Institutions: Ensure that religious and ethnic groups are proportionately represented in state cabinets, civil service, judiciary, and law enforcement to build trust and reduce perceptions of bias.

***3. Foster Interreligious Dialogue and Civic Education***

- Community Dialogues and Peacebuilding Forums: Organize regular town hall meetings, interfaith seminars, and public discussions to dispel misconceptions about religious practices and legal traditions, including Shariah.
- Integrate Civic and Religious Education: Encourage schools and religious institutions to teach civic values such as tolerance, justice, mutual respect, and the importance of peaceful coexistence.

***4. Create Legal Safeguards and Oversight Mechanisms***

- Establish Religious Legal Monitoring Boards: These boards can ensure that the application of religious laws complies with constitutional provisions and does not infringe on fundamental human rights.

***5. Build Media and Public Communication Strategy***

- Peace Journalism and Responsible Media: Train journalists to report sensitively on religious issues, counter hate speech, and promote narratives of unity.
- Government Communication Units on Religious Affairs: State governments can set up public affairs units to handle religious queries, counter misinformation, and offer clarifications on controversial policies.

***6. Invest in Justice Sector Reforms***

- Equip Shariah and Customary Courts: Where religious courts exist, they should be properly staffed, trained, and regulated to uphold fairness and legal professionalism.
- Judicial Training on Plural Legal Systems: Organize seminars and workshops for judges and legal officers on how to navigate and reconcile overlapping jurisdictions between statutory, Shariah, and customary courts.

***7. Encourage Faith-Based Development Initiatives***

- Joint Projects by Religious Institutions: Encourage Muslim and Christian organizations to collaborate on development initiatives—such as healthcare, education, and poverty alleviation—to build social capital and shared community interest.
- Government Partnerships with Religious Bodies: Governments can engage faith-based groups in designing and implementing social welfare programs, which can also reinforce the message of unity through service.

## Conclusion

This study set out to investigate the socio-political implications of the adoption of Shariah law in Western Nigeria, particularly in terms of its impact on religious rights, legal pluralism, and interfaith relations. Drawing primarily on quantitative data gathered through structured questionnaires, supplemented with legal and policy analysis, the findings reveal a complex and often contested landscape.

The analysis indicates that perceptions of Shariah law are strongly influenced by factors such as religious affiliation, professional background, and education level. Among Muslim respondents, especially legal scholars and religious leaders, Shariah is viewed as a legitimate exercise of religious freedom under the Nigerian constitution. Conversely, a significant proportion of Christian respondents and secular professionals expressed concerns over potential encroachments on Nigeria's secular legal identity, fearing that the implementation of Shariah law might lead to religious marginalization or political imbalance.

The study also finds that legal pluralism is generally accepted, but its implementation must be handled carefully to avoid conflict. Support for Shariah law was found to be higher among respondents with lower income levels and among those who perceive the secular judicial system as corrupt or inefficient, suggesting a potential correlation between socioeconomic dissatisfaction and support for alternative legal frameworks.

Furthermore, the findings indicate that knowledge gaps exist among the general population concerning the scope of Shariah law. Many non-Muslim respondents wrongly believed that Shariah law applies to all citizens, a misperception that fuels unnecessary anxiety and resistance. This underlines the need for public education and clearer communication from legal and governmental institutions.

## References

**Abikan, A. I.** 2013. "The application of Shariah in a secular state: The Nigerian experience." *Journal of Islamic Law Studies* 14(2): 112-135.

**Adebanwi, W.** 2004. "The Shariah Debate and the Construction of a 'Muslim' Identity in Nigeria." Journal of Modern African Studies 42(1): 1–22.

**Adegbite, A.** 2020. "Religious pluralism and the Nigerian legal system: Challenges and prospects." *African Journal of Law and Society* 8(1): 45-67.

**An-Na'im, A. A.** 2008. *Islam and the secular state: Negotiating the future of Shariah*. Harvard University Press.

**Benda-Beckmann, F. von.** 2002. "Who's afraid of legal pluralism?" Journal of Legal Pluralism and Unofficial Law 34(47): 37–82. https://doi.org/10.1080/07329113.2002.10756563

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

**Eze, O. C.** 1984. *Human rights in Africa: Some selected problems.* Lagos: Nigerian Institute of International Affairs.

**Ezeilo, J.** 2011. "Women's rights, religion, and legal pluralism in Nigeria". *Journal of African Law* 55(1): 1-21.

**Falola, T.** 2009. *Colonialism and Violence in Nigeria*. Indiana University Press.

**___.** 2018. "Religious politics in Nigeria: A historical perspective." *African Studies Review* 61(2): 78-102.

**Federal Republic of Nigeria [FRN].** 1999. *Constitution of the Federal Republic of Nigeria.* Abuja: Government Press.

**Griffiths, J.** 1986. "What is legal pluralism?" Journal of Legal Pluralism 18(24): 1–55. https://doi.org/10.1080/07329113.1986.10756387

**Hobbes, T.** 1651. *Leviathan.* Oxford University Press.

**Ibrahim, J.** 2004. *The transformation of ethno-religious identities in Nigeria*. In A. B. Zack-Williams, D. Frost, & A. Thomson (Eds.), *Africa in crisis: New challenges and possibilities* (pp. 182–196). Pluto Press.

**Ibrahim, J., and O. Igbuzor.** 2002. "Memorandum to the Presidential Committee on the Review of the 1999 Constitution." Centre for Democracy and Development (CDD).

**Kendhammer, B.** 2013. "The Sharia controversy in Northern Nigeria and the politics of Islamic law in new and uncertain democracies." *Comparative Politics* 45(3): 291–311.

**Kymlicka, W.** 1995. *Multicultural citizenship: A liberal theory of minority rights.* Oxford University Press.

**Last, M.** 1967. *The Sokoto Caliphate*. Oxford University Press.

**Lenta, P.** 2005. "Taking diversity seriously: Religious courts and the constitution of South Africa." Journal for Juridical Science 30(1): 58–73.

**Locke, J.** 1689. *Two treatises of government.* Cambridge University Press.

**Loimeier, R.** 2012. *Islamic Reform and Political Change in Northern Nigeria.* Northwestern University Press.

**Marshall, P.** 2002. *Shariah law and the challenge of religious freedom.* In P. Marshall (Ed.), *Radical Islam's rules: The worldwide spread of extreme Shariah law* (pp. 7–20). Rowman & Littlefield.

**Merry, S. E.** 1988. "Legal pluralism." Law & Society Review 22(5): 869–896. https://doi.org/10.2307/3053638

**Na'Allah, A. R.** 2009. *Ilorin: The journey so far.* Ilorin: Majab Publishers.

**Nmehielle, V. O.** 2004. "Sharia Law in the Northern States of Nigeria: To Implement or Not to Implement, the Constitutionality is the Question." Human Rights Quarterly 26(3): 730–759.

**Nwauche, E. S.** 2010. "Shariah law and the Nigerian constitution: An analysis of conflicts and harmonization strategies". *Journal of Comparative Law in Africa* 2(1): 23-41.

**Oba, A. A.** 2002. "Islamic law as customary law: The changing perspective in Nigeria." International and Comparative Law Quarterly 51(4): 817–850.

**___.** 2011. "The Sharia Court of Appeal in Northern Nigeria: The continuing crisis of jurisdiction." Journal of Islamic Law and Culture 13(1): 29–53.

**Ojo, M.** 2016. "Islam and religious diversity in Nigeria: Debating the introduction of Shariah law in Western Nigeria." *Religious Studies Journal* 19(3): 201-218.

**Olaniyan, A.** 2020. "Shariah Law in Southern Nigeria: A Reappraisal of Constitutionalism and Religious Freedom." Journal of Law and Religion 35(2): 275–290.

**Organization of African Unity.** 1981. "African Charter on Human and Peoples' Rights." https://www.achpr.org/legalinstruments/detail?id=49

**Ostien, P.** 2007. *Sharia Implementation in Northern Nigeria 1999–2006: A Sourcebook* (Vol. I–III). Spectrum Books.

**Paden, J. N.** 2005. *Muslim civic cultures and conflict resolution: The challenge of democratic federalism in Nigeria*. Brookings Institution Press.

**Peters, R.** 2003. "Islamic criminal law in Nigeria: Application and debates." *African Affairs* 102(406): 571-590.

**Rawls, J.** 1971. *A theory of justice.* Harvard University Press.

**Rousseau, J. J.** 1762. *The social contract.* Penguin Classics.

**Supreme Court of Nigeria.** 2006. Kano State Government v. Federation 6 NWLR (Pt. 1005) 581 (Nigeria).

**United Nations.** 1948. "Universal Declaration of Human Rights." https://www.un.org/en/about-us/universal-declaration-of-human-rights

**Uthman, I. O.** 2019. "Islamic law in Nigeria: Historical perspectives and contemporary issues." *Nigerian Journal of Islamic Studies* 11(4): 89-102.

**Yadudu, A. H.** 2000. *Colonialism and the transformation of Islamic law in Northern Nigeria.* Ibadan: University Press.

**Yusuf, A.** 2021. "Public perceptions of Shariah law in Nigeria: A survey analysis." *Journal of African Political Studies* 15(1): 55-79.

**Yusuf, H. O.** 2013. "Colonialism and the judiciary in Nigeria: Unpacking legal history." *African Journal of Legal Studies* 6(2–3): 245–274.

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

# Gaza under British rule (1917-1948): Contradictory Promises and the Colonial Legacy in Palestine

**Bachelor finalist, Mariana RODRIGUES***
**Lt.Col. Cav Pedro FERREIRA, PhD****
*University of Lisbon
e-mail: mrodrigues21@edu.ulisboa.pt
**Portuguese Military Academy Research Centre
e-mail: ferreira.pna@exercito.pt

## Abstract

This paper analyses the impact of British rule in Gaza between 1917 and 1948, highlighting the way in which the commitments made by Britain during the First World War influenced the political configuration of Palestine, specifically the territory of Gaza. The importance of this topic lies in the need to understand the historical origins of geopolitical tensions in the region, and is justified by the significant role of the British administration in articulating contradictory commitments to the Arabs and Jews, which triggered long-lasting conflicts. The main objective is to evaluate the effects of these promises on Gaza and its population, particularly in the context of the British administration. The methodology adopted is historical-analytical, based on bibliographical research and the analysis of books and scientific articles. It concludes that British action has profoundly molded the socio-political reality of Gaza, contributing to territorial fragmentation, the political exclusion of Palestinian Arabs, and the aggravation of identity tensions. This analysis contributes to a critical understanding of the British legacy in Palestine.

**Keywords:**
Gaza; British Mandate; Palestine; Balfour Declaration; Arab nationalism; Zionism; self-determination.

**Article info**
Received: 15 May 2025; Revised: 10 June 2025; Accepted: 13 June 2025; Available online: 27 June 2025

Citation: Rodrigues, M., and P. Ferreira. 2025. "Gaza under British rule (1917-1948): Contradictory Promises and the Colonial Legacy in Palestine." *Bulletin of "Carol I" National Defence University*, 14(2): 154-166. https://doi.org/10.53477/2284-9378-25-21

This article analyses the impact of British rule over the territory of Gaza between 1917 and 1948, in the light of the diplomatic promises made during the First World War. The relevance of this topic is justified by the centrality of Palestine - and Gaza in particular - in the dynamics of conflict and instability that persist to this day. Understanding the historic roots of British involvement sheds light on the genesis of the territorial identity and the political disputes that shaped the 20th century in the Middle East.

The problem we intend to address lies in the contradictions of the promises made by Britain to different actors - Arab leaders and the Zionist movement - and the way how these promises influenced British imperial policy in the region. Specifically, this study asks how these decisions affected the territory of Gaza, both at the level of its political and social structures and in the context of the emergence of local resistance. The importance of this question lies in its direct impact on the development of the Israeli-Palestinian conflict and the construction of clashing national identities.
In recent decades, research into the British Mandate and Palestine has deepened, highlighting themes such as British imperial management, the effects of the Balfour Declaration, Arab resistance, Jewish immigration, and the formation of Zionist institutions.

This article adopts a historical-analytical approach aimed at understanding British actions in Gaza, based on the articulation between primary documentary sources and specialized literature. This approach is appropriate because it allows political decisions to be contextualized in the light of broader historical processes and their consequences to be critically examined.

One of the key concepts in this study is Zionism, understood as the political and ideological movement that was established in the late nineteenth century, advocating for the establishment of a sovereign Jewish homeland, with Palestine regarded as the most suitable location due to its historical and religious significance to the Jewish people. Zionism, as a mobilizing force, gained strength with the support of the Balfour Declaration and was a determining element in the demographic and political transformation of the Palestinian territory.

This article is organized into four main parts. The first presents the historical background to the British promises during the First World War. The second analyses the direct impact of the British Mandate on Gaza. The third examines the Arab-Palestinian reaction, with an emphasis on the Revolt of 1936-1939. Finally, the fourth part deals with the end of the Mandate period with the 1948 war, the creation of the State of Israel, and the massive displacement of Palestinians, many of whom took refuge in Gaza.

The aim of this article is therefore to understand how British rule and its political decisions have shaped the historical trajectory of Gaza and contributed to the

worsening of tensions between Jews and Arabs in Palestine. The central question guiding the study is: how did the promises made by Britain during the First World War and the subsequent administration of the British Mandate affect the territory and population of Gaza? Through this analysis, we aim to contribute to the critical understanding of British colonialism and its legacy in the Middle East.

## British Promises and the Reorganization of the Middle East (1915-1917)

The drawing of a new geopolitical map of Europe and the Middle East marked the end of the First World War. Even before the First World War was due to end, it was already known that Great Britain wanted to keep the Palestinian territory to which Gaza belonged. The Hussein-McMahon Correspondence of 1915 included a series of communications in which the British government pledged to recognize Arab independence, contingent upon Husayn ibn Ali, the Sharif of Mecca and King of Hejaz, initiating a revolt against the Ottoman Empire. The proposed Arab territory was to include regions such as Syria, Mesopotamia, and potentially Palestine (Haidar, et al. 2024).

During the First World War, a confidential exchange of letters took place between Sir Henry McMahon, the British High Commissioner in Egypt, and Sharif Hussein of Mecca, laying the groundwork for British-Arab relations during the conflict. The British desired Sharif Hussein's support in their campaign against the Ottoman Empire during the First World War. As the custodian of the Muslim Holy Places, Hussein was regarded by Britain as a potential unifying figure for the Arab world, especially given his claim to represent the entire "Arab Nation". In return for his commitment to lead an uprising against the Ottomans, Britain offered financial assistance and military guidance, notably through British officers such as T. E. Lawrence, later popularized in the film *Lawrence of Arabia*, and assurances of support for Arab independence. The correspondence between McMahon and Hussein unfolded over several months, with McMahon's letter dated 24 October 1915 generally recognized as the most pivotal document in the exchange. By this time, British ambitions regarding Palestine were already understood (Sabel 2022, 15).

This correspondence gave rise to the Sykes-Picot agreements of 1916, which had a major impact on the region where Gaza was located. But the promise to give the Arabs independence was not fulfilled (Salihu 2024). France and Great Britain, with the consent of Russia, reached a secret agreement during the First World War to divide the territories of the Middle East into respective zones of influence and control following the anticipated defeat of the Ottoman Empire. The French zone would correspond to the current northern Syria and Lebanon, and the British zone would cover southern Iraq and the port of Haifa (Palestine). The agreement also foresaw that Jerusalem, along with certain parts of Palestine, including Gaza, would be placed

under a vaguely defined international administration. The specific nature of this administration was to be determined through consultations with Russia and other allied powers, rather than being directly assigned to British or French control under the initial terms of the agreement. Due to discontent with this decision, Arab nationalist movements emerged (Salihu 2024).

Although this agreement did not assign Gaza or Palestine directly to British control, Britain attacked Gaza in what became known as the First, Second, and Third Battles of Gaza. The British attacks on Gaza were part of the British offensive on the Sinai and Palestine fronts during the First World War, following the Ottoman attempts to seize the Suez Canal. In the first two battles, even with the British superiority in numbers of soldiers, vehicles, weapons, and food, as well as in naval bombardment, the Ottoman forces managed to resist and repel the British attacks (Ağaoğlu 2017). However, in November 1917, in the Third Battle of Gaza, the British managed to conquer Gaza. In these three battles, Gaza suffered intense bombardments that had a significant impact on its population, destroying the city and causing high casualties (Halevy 2015).

Also, in November 1917, the British government issued the Balfour Declaration, motivated by the desire to gain support from influential Jewish communities around the world during the First World War, particularly in the United States and Russia, as well as strategic and imperial interests in the region. Palestine was seen as extremely important for the future security and prosperity of the British Empire (Haidar, et al. 2024).
According to the Balfour Declaration of 1917, His Majesty's Government expressed its support for the establishment of a national home for the Jewish people in Palestine, if this would not prejudice the civil and religious rights of existing non-Jewish communities or Jews elsewhere (Sabel 2022, 47)[1]. This declaration signaled a significant change in British policy towards the future of Palestine, moving away from the idea of an international administration outlined in Sykes-Picot and paving the way for British control to implement the Balfour Declaration (Haidar, et al. 2024).

## The Imposition of the British Mandate and the Gaza Affair (1917-1936)

The question of whether the Balfour Declaration contradicted the McMahon-Hussein Correspondence remains a subject of ongoing debate. The official British stance has consistently maintained that the Balfour Declaration did not pertain to Palestine as covered by the McMahon-Hussein agreement. Some authors claim that the Declaration did not contradict the Sykes-Picot Agreement, since the Declaration was subsequently accepted by France (Sabel 2022, 50). Other scholars contend that the Balfour Declaration

[1] "Balfour Declaration, statement of British support for "the establishment in Palestine of a national home for the Jewish people." It was made in a letter dated November 2, 1917, from Arthur James Balfour, the British foreign secretary, to Lionel Walter Rothschild, 2nd Baron Rothschild (of Tring), a leader of the Anglo-Jewish community" (The Editors of Encyclopaedia Britannica 2025). The original text can be consult in https://avalon.law.yale.edu/20th_century/balfour.asp

conflicted with earlier British promises to the Arabs, particularly those found in the Hussein-McMahon Correspondence of 1915, wherein Britain appeared to support Arab independence in regions including Syria, Mesopotamia, and potentially Palestine (e.g. (Haidar, et al. 2024)).

The Balfour Declaration also raises the question of the principle of self-determination, given that most of Palestine's population in 1917 was Arab. The Palestinians felt betrayed by the Balfour Declaration, as it ignored their aspirations for self-determination (Sabel 2022, 43). The declaration exacerbated tensions between Jewish immigrants and the Arab population, leading to violent clashes over land and resources. Britain was aware that consulting the population could result in an "anti-Jewish verdict but justified its policy with the importance of the Jewish question outside Palestine and the belief in a historical Jewish claim to the region (Sabel 2022, 48). It is also important to note that, in 1917, Britain did not hold sovereign rights over Palestine to cede territory to the Jewish people. The Balfour Declaration constituted a conditional commitment, stipulating that if Britain were to gain rights over Palestine, it would act following the terms outlined in the Declaration. Although the Balfour Declaration affirmed protections for the civil and religious rights of Palestine's non-Jewish inhabitants, it notably omitted any recognition of their collective national identity or political rights (Sabel 2022, 50).

The Balfour Declaration is also considered a fundamental antecedent to the Nakba[2] of 1948 and the creation of the State of Israel. The declaration gave impetus to the Zionist project of establishing a Jewish state in Palestine (Inci n.d.).
This declaration was a turning point for the Zionist movement and contributed to an increase in Jewish immigration to Palestine, which included the Gaza region, and was supported internationally by powers such as France, the United States, Italy, and Japan, which was a gain for the Zionist movement. This declaration is still seen by many Palestinians as the root of their difficulties and as a historical injustice (Inci n.d.).

[2] The Nakba "means "catastrophe" in Arabic, refers to the mass displacement and dispossession of Palestinians during the 1948 Arab-Israeli war" (United Nations n.d.).

After the end of the First World War in 1918, the map of the Middle East was significantly altered with the collapse of the Ottoman Empire, which affected Gaza. The Allied powers, Great Britain and France, began to plan the future of the region, which included the division of the Middle East. The League of Nations, established following the conclusion of the war, played an important role in formalizing the status of Palestine (Martinelli 2022, 89).

In 1919, the United States appointed the King-Crane Commission, or 1919 Intercollegiate Commission on Turkish Mandates, an American

commission of enquiry into the disposition of areas within the former Ottoman Empire, sent to the Middle East by President Woodrow Wilson. The Commission aimed to consult the populations of the Ottoman Empire on their post-imperial territorial and political objectives, compiling their responses in the King-Crane Report, which was only published in 1922 (Cooper and Omicron 2021).

The Commission concluded and recommended that the mandate for Palestine should be given to the United States, noting the strong and unanimous opposition of the Muslim and Christian populations to the Zionist project in Palestine, which was intrinsically linked to the question of Syrian unity. The Commission also proposed the appointment of Emir Feisal as the head of a newly unified Syrian state, asserting that the governance and administration of such a state should be derived from the will and free choice of its native populations. According to the Commission, the concept of a national home did not equate to the establishment of a Jewish state. The Commission warned that such a development could gravely infringe upon the civil and religious rights of Palestine's non-Jewish communities and therefore recommended that Jewish immigration be curtailed and the pursuit of a separate Jewish state be reconsidered. The King-Crane report was not implemented by the US government and had a limited impact on the political decisions of the time (Sabel 2022, 62).

Still in the context of the end of the First World War, the Paris Peace Conference took place between 1919 and 1920, where the victorious Allied powers met to define the terms of peace with the defeated countries and to decide the fate of the territories of the dismembered Ottoman Empire. One of the crucial decisions taken at the Paris Peace Conference was the establishment of the League of Nations Mandate system to supervise the Ottoman territories in the region. Palestine, which included Gaza, was placed under British Mandate following the decisions of this conference, later formalized at the San Remo Conference, chaired by the Supreme Council of the Allies in April 1920, where Türkiye formally ceded Syria, Palestine, and Mesopotamia. The former Ottoman provinces of Syria and Lebanon were mandated to France, Palestine, and Iraq (Mesopotamia) were mandated to Great Britain (Inci n.d.). The authority to determine the status of Palestine rested with the Allied Powers rather than the League of Nations. The Allied Powers were the ones who decided that Great Britain, as the Mandate Power, would govern Palestine following the terms of the agreement between them and the League. As early as August 1920, Türkiye signed the Sèvres Peace Treaty, by which it renounced all its rights over the Ottoman Empire in the Middle East in favor of the Allies. British rule of Gaza and Palestine officially began in 1922 with the British Mandate for Palestine, which was established by the decisions of the Paris and San Remo Peace Conferences and incorporated the Balfour Declaration of 1917 (Sabel 2022, 44).

The League of Nations Mandate for Palestine, which ran from 1922 to 1947, was a crucial period in the history of Palestine, framed by the mandate system established

after the First World War. The League of Nations designed this system to manage the former territories of the German Empire and the Ottoman Empire. Although intended to bring these territories to independence, in practice, the mandate system represented a distinct form of colonialism (Feldman 2008, 6).

Palestine was classified as a Class A Mandate, which, according to Article 22.4 of the Covenant of the League of Nations, meant that its existence as an independent nation could be recognized provisionally, on condition that the advice and help of a mandatary (Great Britain) guided its administration until it was able to conduct itself. However, effective power resided with Great Britain. The Mandate policy, designed to support the establishment of a Jewish national home, had a direct and increasingly significant impact on Gaza, as well as the broader Palestinian territory. It promoted Jewish immigration to Palestine, which in turn intensified tensions and conflicts with the existing Palestinian Arab population in Gaza and other regions (Martinelli 2022, 88).

The British administration, mandated by the decisions of the Paris Peace Conference, had the dual obligation of promoting the Jewish national home and preserving the civil and religious rights of the Arab population, a contradiction that became a source of instability in Gaza and throughout Palestine (Feldman 2008, 240). The governance policies implemented by the British in Gaza, under the Mandate system defined at the Paris Peace Conference, shaped daily life and administration in the region for decades.

The Mandate explicitly referenced Jews, the Jewish population in Palestine, and the broader Jewish community in the region, yet it failed to acknowledge Palestinians or Palestinian Arabs, who comprised approximately 92 percent of the population. Instead, Palestinians were referred to in vague and generic terms such as "non-Jews, "natives," or "peoples and communities," without formal recognition by either the British authorities or the League of Nations (Martinelli 2022, 87).

The Mandate period saw the simultaneous growth of Palestinian nationalism and Zionism, with both claiming the same territory (Martinelli 2022, 13). British policies in the Mandate faced increasing difficulty in reconciling their obligations towards the Zionist movement and the Arab population. The Palestinian political elite sought to maintain their traditional role as interlocutors with the British authorities and the League of Nations, demanding the abrogation of the Balfour Declaration and an end to Jewish immigration (Rigby 2015).

## The Arab Resistance and the rise of the conflict (1936-1939)

The 1930s saw the rise of Palestinian resistance to Zionist colonization, culminating in the Arab Revolt of 1936-1939. The Arab Revolt of 1936-1939 in Palestine was a

period of intense unrest and violence by the Palestinian Arab population against British rule and the growing foundation of a Jewish national home (Martinelli 2022, 98). This uprising represented a significant milestone in the Palestinian nationalist struggle and had profound impacts on British policy towards the region.

This uprising took place because of growing Arab opposition to the Zionist project and Jewish immigration to Palestine (Sabel 2022, 47). The Palestinian Arabs saw Zionism as a threat to their demographic majority and their national aspirations. The increase in Jewish immigration in the 1930s intensified tensions, leading to a growing sense that the future of Palestine was being decided against the will of the Arab population. Of course, the Arab rejection of the British Mandate from its inception, seen as a betrayal of the promises of independence made during the First World War, also contributed to the atmosphere of conflict. The general strike of 1936, one of the main strategies of the uprising, affected Gaza's local economy, which depended on trade and agriculture (Feldman 2008, 21).

The revolt led to a reassessment of British policy towards Palestine. In 1937, the Peel Commission was established and proposed the partition of Palestine into two sovereign states, one Arab and one Jewish. However, the proposal was denied by the Pan-Arab Congress and the British government, which feared alienating Arab allies (Sabel 2022, 83).

In 1939, the British government published the White Paper, which outlined a proposal for the creation of an independent Palestinian state within ten years, while simultaneously imposing limitations on Jewish immigration and land purchases. This policy change was seen by the Jews as a betrayal of the Balfour Declaration, while the Arabs, although initially supportive, realized its limited implementation, leading Zionist leaders to seek support from the United States (Martinelli 2022, 99).

The Arab Revolt of 1936–1939 represented a turning point in the Arab-Israeli conflict, revealing the extent of Arab resistance to Zionist aspirations and prompting shifts in British policy in the region. However, British repression left the Palestinian population exhausted and disarmed, resulting in a weakened leadership. In contrast, the Zionists, more organized, strengthened their military and political institutions (Martinelli 2022, 99). The 1936-1939 Uprising also influenced the anti-colonial struggle in Palestine, including Gaza, serving as a precursor to the later intifadas (Martinelli 2022, 99). The kufiyah[3] became one of the main symbols of Palestinian resistance, and the uprising remains a central element of Palestinian collective memory, something that would continue to be relevant in Gaza in subsequent conflicts (Alghezi 2023).

[3] "Keffiyeh, headdress typically made of cotton and traditionally worn by men in parts of the Middle East. The black-and-white checkered keffiyeh, which represents the Palestinian liberation movement, is also worn to convey political sentiments." (McDonald 2025).

Although the uprising was suppressed, it had lasting consequences on the development of Palestinian nationalism and the redefinition of British policy towards the region, preparing the ground for the events that would culminate in the end of the British Mandate and the 1948 war (Martinelli 2022, 19-20).

## The end of the British Mandate and the consequences for Gaza (1947-1948)

With the end of the Second World War, Britain faced growing international pressure over the question of Palestine. Following this pressure and with the creation of the United Nations (UN) on 29 November 1947, the UN passed Resolution 181, which recommended the partition of Palestine into two separate independent states, but linked by an economic union, one Arab and one Jewish, with Jerusalem being an international zone (*the corpus seperatum*) (Sabel 2022, 93). This resolution was accepted by the Zionists but rejected by the Palestinians (Haidar, et al. 2024).

The resolution proposed ending the British Mandate in Palestine, involving the gradual withdrawal of British forces, and the establishment of borders between the proposed Arab and Jewish states, with Jerusalem receiving special status. The creation of both states was set for completion by October 1, 1948. The plan called for dividing Palestine into eight areas: three for the Arab state, three for the Jewish state, with Jaffa designated as an Arab enclave within Jewish territory, and Jerusalem placed under international oversight by the United Nations Trusteeship Council. The Gaza Strip was also designated as part of the Arab state (Inci n.d.).

The plan allocated roughly 55 percent of Palestine's territory to the proposed Jewish state, even though Jews made up about one-third of the population at the time. The remaining 45 percent was set aside for the Arab state, which included areas with predominantly Arab populations (Salihu 2024). The Jewish Agency in Palestine accepted the Partition Plan, while the Palestinians rejected it, viewing it as unjust and a significant loss of land. They perceived the resolution as taking away most of their territory. The Arab response to UN Resolution 181 was one of outright rejection and opposition (Haidar, et al. 2024).

The rejection of the Partition Plan by the Arab and Palestinian leadership led to an increase in violence and subsequently to the 1948 war. This war, known to Palestinians as Al-Nakba, had a significant impact on Gaza. As a result of the 1948 war, thousands of Palestinians were displaced from their homes, and many of them took refuge in the Gaza Strip. The problem of Palestinian refugees, including those in Gaza, has become a central and enduring issue (Alghezi 2023).

It is important to note that the Partition Plan was never fully implemented due to the 1948 war. The Mandate period ended with the 1948 war and the creation of

the State of Israel in most of the Mandate territory. The failure to create an Arab-Palestinian state, the displacement of a large part of the Palestinian population, and the division of Jerusalem marked the end of this era. Instead of the two states envisaged in Resolution 181, the result of the war was the expansion of Israel beyond the proposed borders, the failure to create an independent Arab state in most of the allocated territory and the division of Palestine between Israel, Jordan (which annexed the West Bank) and Egypt (which administered Gaza) (Alghezi 2023).

Although Resolution 181 did not result in the immediate creation of a Palestinian state in Gaza, it is seen as an initial international recognition of the legitimacy of a Jewish state in Palestine. For Palestinians, the resolution and the subsequent war and displacement, including to Gaza, are foundational events in their history and their struggle for self-determination. This period was marked by growing tensions between Palestinian and Zionist national aspirations, the policy of British support for the creation of a Jewish national home, and culminated in the partition of the territory and the 1948 conflict (Martinelli 2022, 84).

It is also important to highlight in this context Israel's Declaration of Independence, which occurred on 14 May 1948, representing the culmination of decades of Zionist aspirations for a Jewish homeland, and was made by David Ben-Gurion, on the day the British Mandate over Palestine came to an end (Salihu 2024).

Following the British withdrawal, Israel's Declaration of Independence on 14 May 1948 prompted the invasion of regular armies from neighboring Arab states (Inci n.d.). This conflict, known as the Arab-Israeli War of 1948 or the War of Independence, was crucial in ensuring the survival and sovereignty of the State of Israel. The Zionists' aim with the war was to conduct an ethnic cleansing of the territory allocated to them by the UN (Rigby 2015).

The fighting lasted until April 1949, when the Armistice Agreements were formalized between Israel and the Arab countries (Sabel 2022, 26). During the conflict, Israeli forces managed not only to resist but also to expand the territory they controlled beyond the borders proposed in the UN Partition Plan (Sabel 2022, 38).

For the Palestinians, the events of 1948 represented a national catastrophe. Around 700,000 Palestinian Arabs were forced to flee or were expelled from their homes. More than four hundred Arab-majority villages and towns were destroyed or repopulated by Jews (Rigby 2015). Responsibility for this exodus remains a controversial issue. The Israeli narrative argues that many Arabs fled voluntarily or at the request of their leaders, in a context of war. The Palestinian position claims that there were deliberate expulsions, massacres, and terror campaigns organized by Israeli forces to empty the region. The authors argue that both the traditional Israeli narrative of conspiracy and the contemporary Palestinian narrative of expulsion are flawed, emphasizing that the historical reality is far more complex (Gelber 2009).

The result was the collapse of Palestinian society and culture. Thousands of refugees settled in neighboring countries and territories such as the Gaza Strip and the West Bank, multiplying the population of these regions (Haidar, et al. 2024). The population of the Gaza Strip increased during the war due to the arrival of refugees. With the end of the war, Israel came to control more than half of the territory of Mandate Palestine, including West Jerusalem. Jordan annexed the West Bank, while Egypt took over the administration of the Gaza Strip (Martinelli 2022, 109). The Arab state proposed by the UN was never created.

For Israelis, the 1948 war represents the realization of two thousand years of Jewish ambitions for a homeland in the Land of Israel (Weintraub and Gibson 2024). Victory in the war is seen as an existential struggle for survival, imposed by hostile Arab forces. For the Palestinians, the Nakba symbolizes the loss of their homeland, the beginning of a life in exile, the dismemberment of their society, and a collective trauma that continues to shape their identity and resistance to this day.

After the 1948 Arab-Israeli War, the Gaza Strip came under Egyptian administration, which also became home to numerous Palestinian refugees who either fled or were expelled from their lands with the establishment of the State of Israel, drastically increasing the local population. Gaza has become one of the most densely populated places in the world, with serious humanitarian difficulties and dependence on international aid. Without Palestinian sovereignty and under Egyptian administration, the region has become a focus of frustration and resistance, developing a strong national identity and becoming central to the struggles of the Palestinian people (Martinelli 2022, 99).

## Conclusion

Based on the guiding question - *how did the promises made by Britain during the First World War and the subsequent administration of the British Mandate affect the territory and population of Gaza?* - the article has analyzed the political, social, and territorial consequences of the British administration against the backdrop of the contradictory promises made during the First World War. Through a historical-analytical approach, it was possible to observe that British decisions, especially the Balfour Declaration and the implementation of the Mandate, generated a context of fragmentation and persistent tension.

The analysis showed that Gaza, although often treated as peripheral, was deeply affected by imperial dynamics. The city was the scene of decisive battles, the object of exclusionary administrative policies, and the target of a growing process of demographic pressure, especially after the 1948 war. The combination of British support for the Zionist project and the effective denial of Arab political rights created a structural imbalance, contributing to the emergence of Palestinian resistance and the consolidation of a conflict that lasted well beyond the Mandate period.

This entire process reveals the complexity of imperial decisions and promises made in wartime contexts, with repercussions that went beyond the short term. The case of Gaza shows that British colonialism, in trying to reconcile opposing interests without real mechanisms for mediation, not only failed in its declared objectives of stability but also fostered the foundations of a long-lasting conflict.
This study can have relevant applications in the field of Middle Eastern history, post-colonial studies, and international relations by offering a critical reading of the role of imperial power in the genesis of contemporary conflicts. It can also contribute to current debates on historical justice, self-determination, and the decolonization of memory.

The limitations of this work include the scarcity of specific primary sources relating to the direct administration of Gaza during the Mandate, which made it difficult to analyze local governance in greater detail. Furthermore, although it was possible to identify the main political and diplomatic milestones, a more in-depth approach to the daily life of the Gaza population would require other types of sources and methodology.
Several lines of research remain open, including: how did the experience of the Mandate shape Palestinian political culture in Gaza? What role did local leadership play in articulating resistance and negotiation? And how do colonial legacies continue to influence administration and political discourse in the Gaza Strip today?

## References

**Ağaoğlu, Sami.** 2017. "Birinci Dünya Savaşı'nda Gazze Muharebeleri / The Battles of Gaza in World War I." *Journal of History, Culture and Art Research* 6 (2): 307: 307-335.

**Alghezi, Ali.** 2023. *"Gaza: A History of Resistance and Freedom."*

**Balfour, Arthur James.** 1917. "Balfour Declaration 1917." *The Avalon Project*. https://avalon.law.yale.edu/20th_century/balfour.asp.

**Cooper, Hana, and Alpha Eta Omicron.** 2021. "The Voices Left Out: Women and the King-Crane."

**Feldman, Ilana.** 2008. *Governing Gaza: Bureaucracy, Authority, and the Work of Rule, 1917–1967*. Durham: Duke University Press.

**Gelber, Yoav.** 2009. "Israel Studies: An Anthology-The Israeli-Arab War of 1948."

**Haidar, Muayad Tawfiq Akel, et al.** 2024. "The Impact of the Balfour Declaration and the British Mandate on the Loss of Palestine (1917-1948)." In *Studies in Computational Intelligence*, 377-387.

**Halevy, Dotan.** 2015. "The Rear Side of the Front: Gaza and Its People in World War I."

**Inci, Fatima.** n.d. *"Dynamics of May 1948 Arab-Israeli War."*

**Martinelli, Martín Alejandro.** 2022. "*Palestina (e Israel), entre intifadas, revoluciones y resistencia."* Luján: Editorial Universidad Nacional de Luján.

**McDonald, Will.** 2025. "keffiyeh". *Encyclopædia Britannica.* https://www.britannica.com/topic/kaffiyeh.

**Rigby, Andrew.** 2015. "The First Palestinian Intifada Revisited."

**Sabel, Robbie.** 2022. *International Law and the Arab-Israeli Conflict.* Cambridge: Cambridge University Press.

**Salihu, Jacob Tsunda.** 2024. "Historical Foundation of the Israel-Palestine Conflict".

**The Editors of Encyclopaedia Britannica.** 2025. "Balfour declaration." *Encyclopedia Britannica.* https://www.britannica.com/event/Balfour-Declaration.

**United Nations.** n.d. *About the Nakba.* https://www.un.org/unispal/about-the-nakba/ (accessed: 11 June 2025).

**Weintraub, Roy, and Lindsay Gibson.** 2024. "The Nakba in Israeli History Education: Ethical Judgments in an Ongoing Conflict." *Theory & Research in Social Education*: 90–121.

**ACKNOWLEDGEMENTS**

We would like to acknowledge the support of the Military Academy Research Centre (CINAMIL) and the Superior Institute of Social and Political Sciences (ISCSP) at the University of Lisbon, which has been instrumental in the completion of this research.

**FUNDING INFORMATION**

The authors declare that no funding or financial support was received from any organisation, institution, or individual for the research, design, execution, or writing of this work.

**CONFLICT OF INTEREST STATEMENT**

The authors declare no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

**DATA AVAILABILITY STATEMENT**

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analyzed specifically for this research.

**DECLARATION on AI use**

The author confirms that AI tools, including language models such as ChatGPT, Notebooklm and DeepL, were used solely to enhance the writing process, improve readability, and assist with grammar and formatting. All intellectual content, analysis, and critical arguments are the result of the author's original work. The AI tools were not used to generate research findings or substitute independent scholarly work.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# The Role of Civil Society in Strengthening National Preparedness for Modern Security Threats

**Assoc. Prof. Ivan OKROMTCHEDLISHVILI, PhD***

*Sulkhan-Saba Orbeliani University, Tbilisi, Georgia
e-mail: i.okromtchedlishvili@sabauni.edu.ge

## Abstract

In the contemporary world, the evolving nature of warfare extends beyond traditional battlefields to include cyberattacks, information warfare, and other hybrid strategies. Within this complex security landscape, civil society has emerged as an important—yet often under-explored—component of national defense. This paper examines the potential of civil society to enhance national preparedness for modern threats, focusing on case studies from the Baltic States—Lithuania, Latvia, and Estonia—and Georgia. By analyzing legal frameworks, institutional roles, and the integration of civil society into state defense systems, the study identifies legal, administrative, and operational challenges and evaluates the effectiveness of civil society in countering emerging threats. Through comparative analysis, the research highlights best practices in civil-military cooperation and provides policy recommendations to strengthen national resilience. The findings contribute to a deeper understanding of civil society's transformative role in contemporary security strategies, emphasizing the growing importance of inclusive, whole-of-society approaches in an era of multifaceted warfare.

**Keywords:**

civil society; national security; threat preparedness; resilience building; crisis response; societal resilience; hybrid threats; cybersecurity.

**Article info**

Received: 15 May 2025; Revised: 11 June 2025; Accepted: 13 June 2025; Available online: 27 June 2025

Citation: Okromtchedlishvili, I. 2025. "The Role of Civil Society in Strengthening National Preparedness for Modern Security Threats". *Bulletin of "Carol I" National Defence University*, 14(2): 167-199. https://doi.org/10.53477/2284-9378-25-22

# Introduction

The security landscape of the 21st century has undergone a profound transformation, with traditional military threats increasingly supplemented or displaced by more ambiguous challenges that blur the lines between war and peace, military and civilian domains. As articulated in the European Commission's Joint Framework on countering hybrid threats (2016), these evolving security challenges underscore "the need for the Union to adapt and increase its capacities as a security provider, with a strong focus on the close relationship between external and internal security." The vulnerabilities exposed by hybrid threats—combining diplomatic, military, economic, and technological methods—necessitate responses that extend beyond conventional defense mechanisms to incorporate whole-of-society approaches.

## *Conceptual Foundations*

This research operates within several interconnected conceptual frameworks. Civil society encompasses the sphere of collective voluntary action outside the state and market, including non-governmental organizations, community associations, professional bodies, and grassroots movements that contribute to public life (Edwards 2014; Salamon 1994). National preparedness refers to coordinated efforts to prevent, protect against, mitigate, respond to, and recover from threats that endanger a nation's security and stability (Perry and Lindell 2003). Hybrid threats, as defined by the EU Joint Framework, constitute "the mixture of coercive and subversive activity, conventional and unconventional methods… used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare" (European Commission 2016; Hoffman 2007). These threats characteristically exploit societal vulnerabilities and generate ambiguity to hinder effective decision-making. Resilience describes a system's capacity to withstand stress and recover, strengthened from challenges, a quality increasingly recognized as essential in modern security frameworks (Walker, et al. 2004; Norris, et al. 2008).

### *Theoretical Framework*

The evolving nature of security threats has prompted reconsideration of traditional state-centric defense paradigms. Three theoretical approaches particularly inform this study's examination of civil society's role in national security:

Resilience theory emphasizes society's adaptive capacity in facing disruptions, prioritizing systems that can absorb shocks and transform when necessary (Boin and Lodge 2016). This adaptive capacity is distributed across multiple societal layers, with civil society organizations playing crucial roles (Jungwirth, et al. 2023).

The human security approach shifts focus from territorial state security to people-centered security, addressing multidimensional threats to communities and recognizing civil society as both a security referent and provider (Sedra 2022).

The whole-of-society approach acknowledges that contemporary security challenges require coordinated efforts across government, private sector, and civil

society sectors, emphasizing security as a shared responsibility requiring diverse partnerships (Jungwirth, et al. 2023).

***Research Rationale***

This investigation into civil society's security role is justified by several converging factors. First, hybrid threats specifically target societal vulnerabilities, seeking to "undermine fundamental democratic values and liberties" (European Commission 2016). Civil society represents both a potential vulnerability and a critical defense mechanism against such threats. Second, modern security challenges demand responses transcending traditional institutional boundaries—spaces where civil society organizations often already operate. Third, as noted in the EU Framework, many security challenges "originate from instability in the EU's immediate neighborhood" (European Commission 2016). Civil society organizations, with grassroots connections and cross-border networks, offer unique capabilities for early warning and community resilience that complement official structures.

Hybrid threats specifically target societal vulnerabilities, seeking to undermine democratic institutions and civil cohesion through cyberattacks, information warfare, and political subversion. Countries situated on NATO's eastern flank – including the Baltic States and Georgia—are particularly exposed to these tactics due to their geopolitical positioning and shared historical experiences under Soviet rule. The Baltic States – Lithuania, Latvia, and Estonia – offer a mature example of civil-military cooperation, having undergone deep integration into NATO and the European Union. These nations have invested heavily in societal resilience and total defense strategies, including formal mechanisms for civil society engagement in national defense. In contrast, Georgia remains a NATO aspirant with an emerging security architecture that still faces institutional, legal, and political constraints. This contrast offers a valuable comparative framework: the Baltic States serve as models of advanced integration, while Georgia provides insight into the opportunities and challenges of adapting these models in less consolidated democracies.

Analyzing these cases together reveals how different stages of political development and alliance integration affect the design, operation, and effectiveness of civil society's role in national defense. Such comparison also helps identify which elements of successful civil-military partnerships may be transferable across diverse governance contexts.

***Research Objectives and Methodology***

This study aims to:

- Analyze the legal frameworks and institutional mechanisms enabling civil society participation in national security across the selected case studies;
- Identify operational models of civil-military cooperation in responding to hybrid threats;
- Assess challenges and limitations facing civil society engagement in security domains;
- Develop policy recommendations for enhancing government-civil society partnerships in building national resilience.

The research employs qualitative methodology, including:

- Document analysis of legal frameworks, policy documents, and strategy papers
- Case study examination of civil society security initiatives in the Baltic States and Georgia
- Comparative analysis of institutional approaches and operational models
- A written interview with Rimvydas Adomavičius, who contributed to establishing and leadership of Lithuania's Komendantūros system. His insights provide valuable firsthand perspectives on implementation experiences, structural challenges, and practical lessons relevant to civil-military integration. The full transcript is available in Appendix B.

***Methodological Note and Limitations***

While the interview provides important practitioner-level insights, the study acknowledges the limitation of relying on a single stakeholder perspective. Future research will expand the empirical base through additional interviews with policymakers, CSO representatives, and defense officials across the case study countries to enhance analytical depth and triangulate findings.

In support of the case studies, this paper draws upon peer-reviewed academic literature and official policy publications to substantiate observations. For example, critiques of hybrid threat environments are grounded in NATO, EU, and UN literature (European Commission 2016; Kaska, Osula and Stinissen 2023). Civil-military structures like the Estonian Defence League and the Lithuanian Riflemen's Union are evaluated through national law and programmatic reporting (Estonian Defence League n.d.; LRT 2022). Further triangulation was conducted through grey literature, organization websites, and defense ministry publications.

A volunteer defense organization can be considered a civil society organization (CSO) under certain conditions, though not always. The distinction depends on factors such as legal status, autonomy, and relationship with the state. A volunteer defense group typically qualifies as a CSO if it is non-profit, citizen-based, operates independently from formal government command structures, and engages in public interest activities such as preparedness, civic education, or resilience-building. Estonia's Kaitseliit (Defence League) exemplifies a hybrid model: it is composed of voluntary citizens and maintains a strong societal base, yet it operates under the administrative authority of the Ministry of Defence. While not fully independent, its civic ethos, affiliated youth and women's organizations, and public service orientation allow it to fulfill key functions commonly associated with civil society. As such, it is best understood as a quasi-CSO that bridges the domains of state security and civil participation.

Conversely, organizations lose their CSO character when they are structurally embedded within state institutions, operate under direct government command, or have members who are formal reservists or government employees. In these cases, their function may still be important for national defense, but their independence—and thus their qualification as CSOs – becomes compromised.

These definitional distinctions are informed by general principles in civil society literature (Edwards 2014; Salamon and Anheier 1997) and by applied frameworks in security sector research (Loada and Moderan 2015; NATO 2024). They help clarify when volunteer defense organizations function as CSOs and when they evolve into state-linked entities.

This article adopts a flexible, context-sensitive approach, recognizing that conventional Western definitions, which emphasize independence from state structures, may not fully capture the hybrid nature of volunteer defense formations in post-Soviet settings. It includes "quasi-CSOs" such as the Lithuanian Riflemen's Union and Komendantūros, Estonia's Kaitseliit (Defence League), and Georgia's Mazniashvili Legion and Aisi as relevant civil society actors due to their grassroots composition, voluntary nature, and societal roles, even if they operate with state coordination. This categorization, while not conventional, reflects the functional realities of post-Soviet security systems and supports a more inclusive understanding of civil society's contribution to national resilience.

***Structure of the Paper***

Following this Introduction, Section 1 examines the legal and institutional dimensions of civil society engagement in national security across the case study countries. Subsections 1.1.1 through 1.1.3 analyze the Baltic models, including Lithuania's, Latvia's, and Estonia's approaches. Section 1.2 examines Georgia's evolving framework for civil society participation in security, highlighting both innovations and persistent challenges. Section 2 presents policy recommendations for enhancing civil society's constructive role in national security, while the Conclusion Section includes reflections on the transformative potential of inclusive security approaches and directions for future research.

By examining these diverse models of civil society engagement in national security, this research contributes to a deeper understanding of how whole-of-society approaches can enhance resilience against modern hybrid threats, offering valuable insights for policymakers, defense professionals, and civil society leaders alike.

## 1. Civil Society and National Security: Legal and Institutional Dimensions

This section examines the evolving relationship between civil society organizations and national defense structures across the Baltic States and Georgia. As modern security threats increasingly transcend traditional military domains, governments have developed varied approaches to harnessing civil society capabilities for enhanced national resilience. The legal frameworks, institutional mechanisms, and operational models discussed below illustrate diverse pathways for integrating civilian volunteers into security architectures while maintaining appropriate oversight and democratic

principles. A comprehensive comparative analysis of civil society engagement across all four case studies is provided in Appendix A, highlighting key similarities and differences in organizational structures, legal frameworks, and strategic approaches. The analysis begins with the Baltic States' models, which demonstrate more mature integration of civil society into defense planning, before examining Georgia's emerging framework for volunteer participation in national security.

### *1.1 Baltic States*

#### *1.1.1. Lithuania*

*Overview of Civil Society's Role in National Defense*

Lithuania presents a comprehensive model of civil society integration into national defense infrastructure, with a multi-layered approach that combines volunteer militias, conscription, and civilian participation mechanisms. The country's historical experience with occupation and its geopolitical position have shaped a defense doctrine that heavily emphasizes societal resilience and whole-of-society approaches to security.

At the center of Lithuania's civil society engagement in national defense stands the Lithuanian Riflemen's Union (LRU), a state-sponsored volunteer organization that unites citizens dedicated to homeland defense. With nearly 15,000 members as of recent data, the LRU serves as a critical bridge between military structures and civil society. The organization's significance in Lithuania's defense ecosystem was underscored in 2022 when the Lithuanian parliament passed legislation expanding its activities and more deeply integrating it into national defense planning.

The LRU's mandate encompasses both armed and non-violent resistance preparation, with members developing capabilities across diverse fields including sports, culture, citizenship education, IT, communication, medicine, and warfare. This multidimensional approach reflects Lithuania's recognition that modern security challenges require competencies beyond traditional combat skills. The organization places particular emphasis on youth engagement, with approximately 6,000 Young Riflemen participating in educational programs and citizenship development activities (Lithuanian Riflemen's Union n.d.).

In 2024, the Komendantūros (Commandant's Offices) were established - the wartime civilian forces, designed to operate alongside local municipalities during armed conflicts. They incorporate both armed and non-armed civilians with various skills, including those with firearms training, medical expertise, or willingness to assist in territorial defense. This recent initiative aims to attract approximately 10,000 citizens who would participate in up to ten days of training annually (LRT 2024).

According to Rimvydas Adomavičius, one of the early leaders of the Komendantūros system, the establishment emerged from "Lithuania's need to strengthen total defense posture through better civil-military integration." The initial vision was to create a structure serving dual purposes: "ensuring effective mobilization in

crisis and providing rear security operations if needed." This was accomplished by "reorganizing and merging the Military Commandant's Offices with the Military Conscription and Recruitment Service" to create a coherent system functioning effectively in both peacetime and wartime (Adomavičius 2025); see Appendix B for the complete interview transcript).

The system evolved through a regional structure consisting of a headquarters and six regional military commandants in major cities (Vilnius, Kaunas, Klaipėda, Šiauliai, Panevėžys, and Alytus), each responsible for their city and district municipalities. By March 2025, approximately 2,500 citizens had actively joined the commandants, with 250 having completed the Basic Commandant Unit Soldier Course. The organization aims to train 1,000 more members by the end of 2025 (Adomavičius 2025). In May 2025, the effectiveness of the Komendantūros system was further tested during the "Interaction 2025" exercise in Klaipėda. This was the first operational activation of the Klaipėda Military Commandant's Office, which coordinated with the Lithuanian Riflemen's Union, the State Border Guard Service, police, fire and rescue, and other municipal entities. About 500 participants simulated a transition from peace to wartime, including curfew enforcement, area control, object protection, and transport checks. The exercise provided a practical demonstration of how Lithuania's total defense structure, including commandant offices and civil society components, can interact under crisis conditions, underscoring the relevance of these institutions in real-world preparedness scenarios (Lithuanian Armed Forces n.d.).

Adomavičius emphasized that "lessons from Ukraine's experience were instrumental in shaping our approach. The war in Ukraine clearly demonstrated that effective territorial defense requires not only frontline military capabilities but also robust rear-area security, protection of critical infrastructure, and mobilization systems that can rapidly integrate civilian resources into the defense effort. We observed how Ukrainian cities and towns that established effective civil-military coordination were better able to resist and recover from attacks, evacuate civilians, and maintain essential services even under extreme pressure" (Adomavičius 2025).

Key implementation challenges included establishing clear lines of authority and coordination between military and civilian structures, attracting sufficient numbers of patriotic citizens willing to commit to defense preparations while maintaining their civilian lives, and securing adequate resources for training and equipment. Adomavičius notes that each commandant's unit required approximately 12,000 euros for new equipment alone, multiplied across the country's municipalities (Adomavičius 2025).

*Legal Basis for Involvement*

Lithuania has developed a robust legal framework governing civil society participation in national defense, which has evolved significantly in recent years to address emerging security challenges:

**Law on the Lithuanian Riflemen's Union** (Republic of Lithuania 1997)**:** In 2022, the Lithuanian parliament enacted a significant revision of the Law on the Lithuanian Riflemen's Union (LRU), marking a major step toward strengthening the organization's role within the country's national defense architecture. The updated legislation introduced a modernized organizational framework and ensured deeper integration of the LRU into national defense planning. One of the most notable changes was the shift in the LRU's chain of command, placing it under the direct subordination of the government rather than solely under the Minister of National Defense. To enhance coordination and oversight, the law also established an advisory council tasked with guiding and aligning the Union's activities with broader security objectives. Furthermore, the revision formalized the LRU's responsibilities in both armed defense and civil resistance during periods of martial law, clearly outlining its dual role in national security. A particularly innovative aspect of the reform was the introduction of new categories of riflemen: "kinetic riflemen," prepared for armed resistance, and "non-kinetic riflemen," trained for unarmed forms of resistance – reflecting a comprehensive approach to modern defense needs (LRT 2022).

**Regulatory Framework for Komendantūros:** New legislation in 2024 established the wartime civilian force structure, defining eligibility requirements, obligations (including an oath that classifies non-compliance as desertion during wartime), and the relationship between these units and existing military and civilian authorities.
The legal architecture reflects Lithuania's strategic prioritization of "society-wide defense" as articulated by Defense Minister Laurynas Kasčiūnas, who has been instrumental in advancing many of these initiatives. This approach draws explicitly from Ukraine's experience during Russia's full-scale invasion, demonstrating how lessons from contemporary conflicts are being rapidly incorporated into Lithuania's civil-military legal frameworks (LRT 2024).

*Government-CSO Cooperation Mechanisms*
Lithuania has established several formal mechanisms for coordinating between government institutions and civil society organizations involved in defense:

**Governance Structure of the Lithuanian Riflemen's Union:** The 2022 legal reforms shifted the LRU's subordination from the defense minister to the government as a whole, creating a more integrated approach. An advisory council was established to coordinate LRU activities, address strategic issues, assess performance, and issue recommendations. This structural change reflects recognition of the cross-cutting nature of modern defense challenges that extend beyond traditional military domains.

**Integration into Defense Planning:** The revised legal framework created what parliamentary Committee on National Security and Defence chairman Laurynas Kasčiūnas described as "a very clear algorithm" whereby the commander of the Riflemen's Union notifies the chief of defense about riflemen capabilities for second-line functions such as facility protection, counter-sabotage operations, and

territorial defense (LRT 2022). This mechanism ensures that civil society capabilities are formally incorporated into military planning processes.

**Training and Readiness Development:** The legislation provides for establishing a dedicated training center to improve riflemen's readiness, institutionalizing knowledge transfer between military professionals and civilian volunteers. Similarly, the Komendantūros system designates the National Defence Volunteer Forces (KASP) as responsible for training civilian participants, creating structured pathways for skills development (LRT 2022; LRT 2024).

**Educational Programs:** The Riflemen's Union implements citizenship and defense skills courses for ninth-grade students throughout Lithuania, demonstrating how civil society organizations serve as conduits for defense awareness in educational settings. These programs represent a systematic approach to cultivating defense consciousness from an early age (Lithuanian Riflemen's Union n.d.).

**Resource Allocation:** The Lithuanian military is legally obligated to provide equipment (weapons, ammunition, protective gear, first aid kits) to citizens assigned to armed units of Komendantūros, ensuring that civil participation is materially supported rather than merely symbolic (LRT 2024).
The relationship between the Komendantūros wartime civilian forces and traditional military structures is "complementary, with clear delineation of responsibilities," according to Adomavičius. The most effective mechanisms for facilitating cooperation included establishing a clear organizational structure where regional commandants oversee municipal commandants, creating a chain of command that parallels civilian administrative divisions. This territorial alignment made coordination with local governments more intuitive. Joint planning processes with municipal administrations for mobilization, protection of important facilities, and other contingency plans "forced both military and civilian authorities to understand each other's capabilities and constraints." Additionally, involving the Lithuanian Riflemen's Union served as a bridging organization between purely civilian volunteers and military personnel, bringing "both paramilitary capabilities and civilian connections that proved invaluable" (Adomavičius 2025).

Regular training exercises involving both military personnel and civilian volunteers created shared experiences and mutual understanding that proved essential for building trust between the different components of Lithuania's total defense approach. The system creates what Adomavičius describes as "a conduit through which civilian capabilities and resources can be integrated into defense planning" (Adomavičius 2025).
The Lithuanian case illustrates a highly evolved model of civil-military integration, where the boundaries between professional military forces, organized volunteer structures, and broader civilian participation have become increasingly fluid. This approach maximizes defense capabilities without proportional increases in standing

military forces, while simultaneously strengthening societal resilience through civic participation and defense education.

The country's ambitious targets – growing Riflemen's Union membership from approximately 15,000 to 50,000 following the 2022 legal reforms and attracting 10,000 citizens to the newly established Komendantūros – demonstrate Lithuania's commitment to significantly expanding civil society's role in national defense (LRT 2022). This expansion reflects both strategic calculation regarding the country's geopolitical position and a recognition that modern security challenges require whole-of-society responses.
However, while innovative, the Komendantūros model remains limited in scale, with only 2,500 trained citizens as of March 2025, compared to its ambitious goals, and its long-term success hinges on sustained state funding and public volunteerism.

*1.1.2. Latvia*

*Key CSO Initiatives*
Latvia represents a compelling case study of civil society integration into national defense infrastructure, with the Ministry of Defence (MoD) maintaining formalized partnerships with various non-governmental organizations. These partnerships serve multiple strategic functions: informing public discourse on security and defense policies, facilitating research on defense-related issues, preserving military heritage, and strengthening public support for the National Armed Forces.
The Zemessardze (Latvian National Guard), while technically a component of the National Armed Forces rather than an independent CSO, serves as a crucial bridge between military structures and civil society. It functions as a volunteer territorial defense organization that enables civilians to contribute directly to national defense while maintaining their civilian occupations. This model exemplifies the "citizen-soldier" concept that has become increasingly relevant in contemporary security environments facing hybrid threats.

Beyond the formal structure of the National Guard, Latvia's defense ecosystem demonstrates a diversified civil society engagement, structured around specific functional domains. Military and veterans' associations – including the Latvian Officers Association, the Latvian Reserve Officers Association, the Association of Latvian National Soldiers, the Union of Latvian National Partisans, and the Latvian Riflemen Association – serve not only commemorative and representational purposes but also contribute to the societal anchoring of defense values. Research and policy organizations such as the Latvian Transatlantic Organisation, the Latvian Institute of International Affairs, the Centre for East European Policy Studies, and the Baltic to Black Sea Alliance facilitate strategic dialogue, promote Euro-Atlantic integration narratives, and generate expertise for both policymakers and the public. Historical memory and identity-building are reinforced through actors like the Brothers' Cemetery Committee, while civil education initiatives, exemplified by the

Latvia's Rural Library Support Association, enhance community-level awareness and engagement. International organizations, notably the Konrad Adenauer Foundation, provide normative guidance and capacity-building, reinforcing Latvia's democratic security culture.

These organizations perform varied but complementary roles within Latvia's broader security architecture. Veterans' groups, for instance, play a prominent role in commemorative events such as the Christmas Battles, Lāčplēsis Day (Freedom Fighters' Remembrance Day), and the January Barricade Days – events that reinforce national identity and collective memory, which are key elements of resilience against disinformation and foreign influence operations.
Research-oriented CSOs enhance analytical capacity by producing independent studies on defense and security, shaping informed public debate, and facilitating international cooperation and knowledge transfer – thereby supplementing state capabilities.

*State Strategy for Resilience and Civil Engagement*
Latvia's approach to civil society engagement in national resilience demonstrates several strategic dimensions:

**Formal Partnership Framework:** The Ministry of Defence has established structured cooperation mechanisms with CSOs, including delegation agreements that formalize responsibilities and expectations. For example, the Brothers' Cemetery Commission operates under a delegation agreement to locate and maintain burial sites of Latvian soldiers killed in world wars in the Russian Federation – an activity with both commemorative and diplomatic significance (MoD n.d.).

**Intergenerational Knowledge Transfer:** Latvia strategically employs veterans' organizations to transmit military experience and values across generations. These organizations conduct patriotic educational events for youth, creating continuity in defense awareness and preparedness. This approach builds long-term societal resilience by embedding defense consciousness in new generations (MoD n.d.).

**International Networking:** Latvia's defense establishment actively promotes CSO participation in international forums and initiatives. The Ministry's partnership with the German Marshall Fund of the United States exemplifies this approach, enabling Latvian NGOs to implement international projects and participate in high-level discussions on transatlantic cooperation and security policy. The Ministry supports the annual Brussels Forum organized by the Fund, connecting Latvian stakeholders with influential international actors across politics, business, academia, and media (MoD n.d.).

**Targeted Historical Commemoration:** The Latvian approach integrates historical memory work into its resilience strategy, with CSOs conducting inspections of

soldiers' burial locations and organizing commemorative events for significant historical battles. These activities strengthen national identity and promote social cohesion – essential components of societal resilience against information warfare and hybrid threats (MoD n.d.).

The Latvian case demonstrates how smaller states with limited resources can enhance their security posture by systematically integrating civil society organizations into national defense frameworks. This approach multiplies defense capabilities without proportional increases in state expenditure while simultaneously strengthening societal resilience through civic participation and education. However, challenges remain in ensuring sustainable funding for CSO activities and maintaining the balance between state guidance and CSO independence – issues that warrant further comparative analysis with other Baltic and Eastern European states.

*1.1.3. Estonia*

Estonia presents a distinctive model of civil society engagement in national defense, one that has been shaped by both the country's historical experience and its pioneering identity as a digital society. The Estonian approach combines traditional volunteer defense structures with innovative cyber capabilities, creating a comprehensive framework for societal resilience against both conventional and emerging threats.

*Role of the Estonian Defence League (Kaitseliit)*

The Estonian Defence League (Kaitseliit) stands as one of the most comprehensive examples of civil-military integration in contemporary Europe. Operating under the authority of the Estonian Ministry of Defence, the organization is structured according to military principles while relying fundamentally on "free will and self-initiative" to enhance national readiness for defense. This balance between military functionality and civic voluntarism represents a defining characteristic of Estonia's approach to civil defense.

The Kaitseliit traces its origins to November 11, 1918, when it was established as a self-defense organization during Estonia's struggle for independence. Following the restoration of Estonian independence in 1991, the Defence League was reconstituted and has since evolved into a significant component of the country's total defense concept. Its status as a legal person governed by public law under the Estonian Defence League Act provides a robust foundation for its activities and ensures appropriate oversight mechanisms (Riigikogu 2013).

With approximately 18,000 direct members and a total of over 29,000 volunteers when affiliated organizations are included, the Defence League represents a substantial mobilization of civil society for defense purposes in a country of just 1.3 million inhabitants. This extensive participation demonstrates the deeply embedded nature of defense consciousness within Estonian civil society (Estonian Defence League n.d.).

The organizational structure of the Defence League reflects Estonia's territorial administration, with 16 districts generally corresponding to the country's county boundaries. This regional approach ensures that defense capabilities are distributed throughout the national territory rather than concentrated in strategic locations, thereby enhancing resilience against various forms of attack and providing for localized response capabilities (Estonian Defence League n.d.).
One of the most distinctive aspects of the Estonian model is its inclusive approach to civil defense through affiliated organizations:

**Women's Voluntary Defence Organization (Naiskodukaitse):** With almost 4000 members across Estonia, this women's organization focuses on involving women in national defense and enhancing broader societal safety. Its training structure is highly systematic, encompassing basic training, professional training, refresher training, and specialized instructor preparation. Members can participate in military defense directly through units assembled by the Defence League or contribute to civil protection initiatives. The organization emphasizes lifelong learning and accommodates members at different life stages – from students to working professionals to retirees – ensuring continuous engagement of female citizens in defense activities (Estonian Defence League n.d.).

**Youth Organizations:** The Home Daughters (Kodutütred) and Young Eagles (Noored Kotkad) serve as pathways for integrating younger citizens into national defense consciousness. Established in the 1930s and revived in 1989, these organizations provide Estonian youth with opportunities for self-fulfillment through patriotic education. Their activities focus on hiking skills, national defense awareness, safety issues, sports, civic skills, and historical knowledge. The training system includes rank advancement tests and specialized skill development, creating a tiered approach to youth development. These organizations effectively function as preparatory structures for future adult participation in defense activities while simultaneously cultivating values of volunteerism and civic responsibility (Estonian Defence League n.d.).

The Estonian Defence League's approach is guided by philosophical principles that emphasize the power of individual conviction over formal military might, as reflected in the Confucian quote prominently featured in their materials: "A commander of great military forces may be defeated. A simple countryman with a belief is invincible." This encapsulates Estonia's recognition that national resilience ultimately depends on the commitment of ordinary citizens rather than solely on professional military capabilities.

*Cyber Defense Unit as Civil-Military Model*
Estonia's experience with sophisticated cyber-attacks in 2007 – among the first coordinated digital assaults against a nation-state – catalyzed the development of innovative approaches to cyber defense that leverage civil society expertise. Estonia's

Cyber Defence Unit (Küberkaitse Üksus) within the Defence League represents a globally recognized model for civil-military cooperation in the digital domain.
The Cyber Defence Unit exemplifies Estonia's adaptation of traditional volunteer defense concepts to contemporary threats. Operating as a specialized component of the Defence League, it brings together civilian IT professionals who volunteer their expertise for national security purposes. This structure allows Estonia to mobilize highly specialized technical skills that would be difficult to develop and maintain exclusively within military structures.

Key aspects of this civil-military model include:
**Volunteer Expertise:** The unit draws upon IT specialists, programmers, cybersecurity professionals, and digital infrastructure experts who maintain their primary employment in the private sector or academia while volunteering their specialized skills for defense purposes. This approach provides Estonia with access to cutting-edge expertise that continuously evolves through participants' professional development in their civilian roles (Kaska, Osula and Stinissen 2023).

**Network Defense Focus:** The unit's primary mission involves protecting critical national information infrastructure and supporting cyber defense during crises. Members can be activated during cyber emergencies to augment government capabilities, providing surge capacity during incidents that exceed the resources of permanent state structures (Kaska, Osula and Stinissen 2023).

**Knowledge Transfer:** The unit facilitates bidirectional knowledge exchange between public and private sectors, helping to disseminate best practices across Estonia's digital ecosystem. This improves overall national cyber resilience by raising standards across sectors rather than concentrating expertise solely within government agencies (Kaska, Osula and Stinissen 2023).

**Training and Exercises:** Regular training sessions and participation in national and international cyber defense exercises ensure that volunteers maintain operational readiness while continuously upgrading their skills. These activities simultaneously strengthen personal networks among participants, creating social infrastructure that can be rapidly mobilized during crises (Kaska, Osula and Stinissen 2023).

**Legal and Ethical Framework:** The unit operates within clearly defined legal parameters that address complex questions related to civilian participation in defensive cyber operations. This provides members with necessary protections while ensuring appropriate oversight (Kaska, Osula and Stinissen 2023).

The Estonian approach to cyber defense demonstrates how traditional concepts of territorial defense can be reimagined for the digital domain. By creating structures that facilitate civilian expert participation in national cyber defense, Estonia has expanded the conventional understanding of civil-military cooperation to

encompass new threat vectors. This model has proven particularly valuable for smaller states with limited resources, as it multiplies defensive capabilities without requiring proportional increases in permanent government personnel.

Estonia's integration of both conventional volunteer defense structures and innovative cyber defense units under the Defence League umbrella represents a holistic approach to modern threats. This model recognizes that contemporary security challenges span both physical and digital domains, requiring defense frameworks that can seamlessly operate across these boundaries. By facilitating structured civil society participation in both domains, Estonia has developed a comprehensive approach to national resilience that addresses the full spectrum of potential vulnerabilities (Kaska, Osula and Stinissen 2023).
The Estonian case illustrates how smaller states can leverage civil society engagement to enhance their security posture against both conventional and emerging threats. By creating legal frameworks and organizational structures that facilitate civilian participation in defense activities – ranging from traditional territorial defense to cutting-edge cyber operations – Estonia has developed a model that maximizes national resilience while maintaining democratic values and civilian oversight.

### *1.2. Georgia*

*Legal and Strategic Provisions for Civil Society Engagement*

Georgia has recently formalized its approach to civil society participation in national defense through strategic legislation. The Defense Code of Georgia, adopted in 2023, establishes a comprehensive framework for "organization of defense based on the total defense approach, strengthening national resilience, organizing national resistance and mission command" (Parliament of Georgia 2023, Art. 2). This represents a significant development in Georgia's security architecture, as it specifically creates legal provisions for volunteer participation in the defense sector.
Chapter XVII of the Defense Code is particularly noteworthy as it explicitly defines "volunteering in the defense sector" as "the voluntary, unpaid training of a natural person in defense and security issues within the organizational framework established by this Code and relevant legal acts, and the use of their skills in the defense sector if needed" (Parliament of Georgia 2023, Art. 166). This legislative foundation provides legitimacy to civil society organizations (CSOs) operating in the defense sphere and establishes parameters for their activities.

The Code stipulates that "the state promotes the organization of volunteering" (Parliament of Georgia 2023, Art. 166.3), demonstrating official recognition of the value that civil society brings to national security. Furthermore, it outlines the creation of a legal entity of public law within the Ministry of Defense system specifically for "coordinating and controlling the implementation of volunteer activities" (Parliament of Georgia 2023, Art. 169.1), institutionalizing the relationship between the state and defense-oriented CSOs.

*Examples of Local CSOs in Defense Preparedness*

*Mazniashvili Legion*

One of the most prominent volunteer civil society organizations in Georgia is the "Mazniashvili Legion," founded in 2013 (though its conceptual foundations date back to 2007). The organization describes itself as a "voluntary and apolitical organization based on a national worldview, uniting everyone who wants to strengthen the defense forces and state structures" (Mazniashvili Legion n.d.). Its training methodology draws from British Armed Forces light infantry and volunteer training programs.

The Legion has set forth a series of strategic objectives that reflect its growing role in Georgia's national defense landscape. Central to its mission is the provision of initial military training for citizens, aimed at enhancing individual preparedness and contributing to a broader culture of defense readiness. A key component of the Legion's structure is the formation of volunteer "Local Defense Units," which operate under the framework of the national Defense Forces, serving as a grassroots extension of state security. To facilitate its activities and ensure nationwide engagement, the Legion is actively working to establish local organizations across Georgia. Beyond its military focus, the Legion also seeks to prepare the population for extreme situations and crises, promoting civil resilience in the face of natural and man-made threats. Importantly, the organization places significant emphasis on the patriotic education of youth, fostering a sense of national identity and civic responsibility among the next generation (Mazniashvili Legion n.d.).

With approximately 1,600 members as of 2023, the Legion has trained thousands of citizens in various defense-related courses and formats. It has a sophisticated organizational structure with five main directions and corresponding departments, plus specialized sections including medical, mining, engineering, drones, hiking, communications, topography, and military history (Mazniashvili Legion n.d.).

The Legion's activities gained official recognition in January 2024 when the legal entity of public law (LEPL) "Volunteer" of the Ministry of Defense was launched, aligning with the organization's long-term vision dating back to 2007. This development followed the Parliament's approval of the Defense Code in late 2023, which formally introduced the concept of a "defense volunteer" in Georgian legislation.

*Aisi*

Another significant organization is "Aisi," which was ideologically formed in 2008 after the Russo-Georgian war and officially registered in 2009. Aisi's mission is "to increase Georgia's civil defense capabilities and popularize volunteer work" (Aisi n.d.). The organization emerged as a response to the recognized gaps in the country's ability to respond to disasters and threats without full civil society involvement.

Aisi conducts two-month free military-camping courses and has trained over 1,000 volunteers in skills including topography and navigation, first aid, trench preparation, forest camping, hiking, and rock climbing. The organization has been cooperating with the Ministry of Defense since its establishment, with formal memoranda of

understanding signed in 2016 and 2021, indicating progressively closer cooperation with state defense structures (Aisi n.d.).

*Challenges: Evolving State-Civil Society Relations, Legal Ambiguity, Lack of Funding*
Despite recent legislative progress, civil society organizations involved in defense preparedness in Georgia face several challenges:
**Evolving State-Civil Society Relations:** While Georgia has made significant progress in formalizing civil society's role in defense preparedness, the relationship continues to develop. The Defense Code establishes oversight mechanisms requiring Ministry approval for volunteer organization status (Parliament of Georgia 2023, Art. 168), which can be interpreted as both a quality control measure and a potential limitation. This regulatory framework reflects the sensitive nature of defense activities and the government's responsibility to ensure proper coordination in security matters, rather than necessarily indicating mistrust. The Ministry's involvement may serve to harmonize civil society efforts with national defense strategy while providing legal protection and recognition for these organizations. However, finding the optimal balance between necessary oversight and operational flexibility for CSOs remains an ongoing process in Georgia's evolving security landscape.

**Legal Ambiguity:** Although the Defense Code creates a framework for volunteering, there remain areas of uncertainty regarding implementation. For example, Article 170.3 states that volunteer organizations may cooperate with municipalities, private entities, and NGOs "in agreement with" the Ministry's public legal entity, potentially creating bureaucratic hurdles. Additionally, the Code stipulates that volunteer registry information "is internal information of the Ministry... and does not belong to public information" (Parliament of Georgia 2023, Art. 172.7), which may limit transparency.

**Lack of Funding:** While the Defense Code allows the Ministry to "issue a grant to the legal entity of public law... /volunteer organization to achieve a specific goal" (Parliament of Georgia 2023, Art. 169.2), sustainable funding remains a challenge. Organizations like the Mazniashvili Legion emphasize that their activities are free to participants, noting "the Legion is not an organization with political goals or for commercial gain" (Mazniashvili Legion n.d.). This commitment to free service, while noble, creates financial sustainability issues. Furthermore, volunteer organizations bear considerable financial responsibilities, including obligations to "compensate a third party for damage caused" and to "compensate a member of the organization/ volunteer for damage caused to them due to deterioration of health" (Parliament of Georgia 2023, Art. 170.4). Without sufficient funding sources, these requirements may create substantial financial burdens for CSOs.
It is important to note that the civil society organizations discussed—such as the Mazniashvili Legion and Aisi—occupy a hybrid space between traditional, independent CSOs and state-coordinated structures. While grounded in grassroots volunteerism, they operate with varying degrees of cooperation or oversight by the

Ministry of Defense. Therefore, referring to them simply as CSOs requires nuance. These are better understood as quasi-CSOs or state-affiliated volunteer formations.
Furthermore, Georgia's political context presents a complex landscape for civil society engagement. On one hand, the government has actively supported initiatives that promote patriotic volunteerism and civic preparedness as part of its total defense vision. On the other hand, some independent NGOs—particularly those involved in governance monitoring and foreign-funded advocacy—have expressed concerns about proposed regulatory changes and public discourse that may impact their operational space (Freedom House 2025; European Parliament 2024). This dual trend—of encouraging civic involvement in defense while reassessing the role of traditional watchdog organizations—warrants careful observation when evaluating the broader inclusiveness and sustainability of Georgia's whole-of-society approach to national security.

## 2. Policy Recommendations

Drawing from the experiences of Lithuania, Latvia, Estonia, and Georgia, several key policy recommendations emerge for enhancing civil society's role in national preparedness against modern security threats. These recommendations are informed by both comparative analyses of the case studies and firsthand implementation experiences shared by practitioners, with particularly valuable insights drawn from the interview with Rimvydas Adomavičius documented in Appendix B. The recommendations aim to strengthen institutional frameworks, improve training programs, foster public-private partnerships, and promote inclusive approaches to national resilience.

### *2.1. Enhancing Institutional Frameworks for CSO Engagement*

The case studies demonstrate that effective civil society participation requires robust institutional and legal frameworks. Governments should:

- Establish clear legal foundations for civil-military cooperation, similar to Lithuania's Law on the Lithuanian Riflemen's Union and Georgia's Defense Code, which formalize the role of volunteer organizations while providing necessary oversight.
- Create coordinating mechanisms between defense institutions and CSOs, following Estonia's model, where the Defense League operates as a legal entity under public law with specific governance structures that balance military functionality with civic voluntarism.
- Develop advisory councils like Lithuania's approach for the Riflemen's Union, enabling systematic coordination between government institutions and civil society organizations while addressing strategic issues.
- Formalize delegation agreements that clearly delineate responsibilities between state actors and CSOs, as seen in Latvia's framework with veterans' organizations and historical preservation groups.

- Balance oversight with independence by designing frameworks that provide necessary supervision without stifling the initiative and flexibility that make civil society contributions valuable. The case of Georgia — still in the early stages of implementation — illustrates the risks posed by excessive control mechanisms, which may undermine trust and effectiveness.

*2.2. Investing in Civil Preparedness Training*

Training programs represent a critical component for building meaningful civil society capacity in national defense:

- Establish dedicated training centers for civil defense volunteers, following Lithuania's approach of creating specialized facilities to improve riflemen's readiness and institutionalize knowledge transfer between military professionals and civilian volunteers.
- Develop comprehensive, multi-domain training curricula that address both traditional defense skills and emerging threat areas, as demonstrated by Estonia's Defense League programs that span conventional territorial defense, medical support, communications, and cyber defense.
- Incorporate civil preparedness into educational systems, building on Lithuania's citizenship and defense skills courses for ninth-grade students and Estonia's youth organizations that provide structured pathways for integrating younger citizens into national defense consciousness.
- Create tiered training systems that accommodate various levels of commitment and prior experience, similar to Estonia's Women's Voluntary Defence Organization model that includes basic training, professional training, refresher training, and specialized instructor preparation.
- Ensure sustainable funding for training programs, addressing the challenges faced by organizations like Georgia's Mazniashvili Legion that provide free training to citizens but risk facing problems with financial sustainability due to their commitment to providing services without charging participants.

Lithuania's Komendantūros system offers valuable insights into effective training methodologies for civilian defense participants. Adomavičius explains that their approach was designed around several core principles. First, they developed a Basic Commandant Unit Soldier Course providing essential military knowledge and skills in a condensed format. Second, they leveraged the expertise of the National Defense Volunteer Forces to deliver training, ensuring professional military standards while recognizing the part-time nature of volunteers' commitment. Third, they focused training on specific wartime tasks related to rear security, protection of important facilities, and support to mobilization rather than attempting to create fully combat-ready units (Adomavičius 2025).

To balance military skills development with civilian career demands, the Komendantūros limited annual training requirements to 3-10 days per year, scheduled training to coincide with exercises involving other reserve components, tailored assignments based on individuals' civilian skills and qualifications, and

created a progressive training system that built competencies over time rather than requiring intensive initial training. They also established more accessible health and physical requirements compared to regular military service, opening participation to a broader segment of society who might otherwise be unable to contribute to defense efforts (Adomavičius 2025).

*2.3. Encouraging Public-Private Partnerships in National Defense*

The examples highlight the importance of leveraging diverse societal resources through public-private partnerships:

- Develop frameworks for mobilizing specialized civilian expertise during crises, modeled on Estonia's Cyber Defence Unit that enables IT professionals to volunteer their skills while maintaining their primary employment in the private sector.
- Create mechanisms for bidirectional knowledge exchange between public and private sectors, facilitating the transfer of best practices across national security ecosystems, as seen in Estonia's approach to cyber defense.
- Establish partnerships with research and academic institutions, following Latvia's cooperation with organizations like the Latvian Institute of International Affairs and the Centre for East European Policy Studies, which supplement state analytical capacity.
- Integrate private sector capabilities into defense planning, allowing for what Lithuania describes as "a very clear algorithm" whereby civilian capabilities are formally incorporated into military planning processes.
- Develop liability and compensation frameworks that address concerns about potential damages, taking note of Georgia's current implementation, where volunteer organizations bear considerable financial responsibilities, which highlights the need for sufficient funding mechanisms.

The Lithuanian experience demonstrates effective strategies for attracting and retaining civilian participants in defense structures. Adomavičius identifies several successful approaches implemented in the Komendantūros system. First, they appealed to patriotism and civic duty, with public messaging emphasizing that the system provides a concrete way for citizens to contribute to national defense without necessarily joining professional military or volunteer forces. This approach was supported by public opinion research showing that more than half (52 percent) of Lithuania's citizens would be willing to contribute to armed resistance during aggression against Lithuania (Adomavičius 2025).

Second, they created a tiered approach to involvement, allowing citizens to participate according to their capabilities, time availability, and commitment level—a flexibility crucial for attracting professionals who could not commit to more intensive military service. Third, they provided meaningful training that developed not only military skills but also emergency management capabilities useful in civilian contexts, making the training more immediately relevant. To maintain engagement during

peacetime, they organized regular training events that created a sense of community and purpose, integrated commandant units with the National Defense Volunteer Forces for training, emphasized the protection of participants' own communities and important local facilities, and created pathways for advancement and recognition within the system (Adomavičius 2025).

*2.4. Promoting Inclusive National Resilience Strategies*

Effective national resilience requires broad participation across demographic groups:

- Design structures that accommodate diverse forms of contribution, similar to Lithuania's differentiation between "kinetic riflemen" for armed resistance and "non-kinetic riflemen" for unarmed resistance, ensuring that citizens with different capabilities and preferences can participate.
- Create dedicated pathways for women's participation in defense activities, building on Estonia's Women's Voluntary Defence Organization model that involves women across different life stages—from students to working professionals to retirees.
- Develop youth engagement programs that cultivate values of volunteerism and civic responsibility from an early age, following the examples of Estonia's Home Daughters and Young Eagles organizations and Latvia's patriotic educational events for youth.
- Leverage veterans' organizations for intergenerational knowledge transfer, as seen in Latvia's strategic employment of veterans' groups to transmit military experience and values across generations.
- Incorporate historical commemoration into resilience strategies, recognizing how Latvia's integration of historical memory work strengthens national identity and promotes social cohesion, essential components of societal resilience against information warfare and hybrid threats.

These policy recommendations reflect the growing recognition that modern security challenges require whole-of-society responses that extend beyond traditional military domains. By enhancing institutional frameworks, investing in training, fostering public-private partnerships, and promoting inclusivity, nations can significantly strengthen their preparedness for the complex and multi-dimensional security threats of the contemporary era.

Based on Lithuania's experience, Adomavičius offers several recommendations for countries developing similar civil society integration into defense structures. He emphasizes building on existing institutions rather than creating entirely new ones, noting that Lithuania's success partly stemmed from merging and reorganizing existing military offices and services. Creating clear territorial alignment between military and civilian administrative structures facilitates coordination and local ownership. Developing flexible participation models that accommodate varying levels of citizen commitment maximizes societal involvement. He recommends focusing on realistic wartime tasks that civilians can perform with limited training,

such as protecting local infrastructure, supporting mobilization, and facilitating civil-military coordination. Adomavičius identifies the most transferable elements of the Lithuanian model as the regional commandant structure that bridges national military and local civilian authorities, the incorporation of existing civil society organizations, the dual peacetime/wartime function of commandant's offices, the focus on local defense and protection of familiar territory, and the graduated training system that builds capabilities over time (Adomavičius 2025).

## Conclusion

***Summary of Key Findings***

This study has examined the evolving role of civil society organizations in strengthening national preparedness against modern security threats, with particular focus on the Baltic States and Georgia. Several key findings emerge from this comparative analysis.

First, the legal and institutional frameworks enabling civil society participation in national security vary significantly across the examined countries. As summarized in Appendix A, while Estonia and Lithuania have developed robust, formalized mechanisms for integrating civil society into defense planning—exemplified by Estonia's cyber defense volunteer units and Lithuania's well-established Riflemen's Union—Latvia and Georgia demonstrate more nascent approaches, though with increasing recognition of civil society's potential contributions.

Second, successful civil-military cooperation models share common elements despite their contextual differences: clear legal mandates, dedicated funding streams, structured training programs, and institutional respect for civil society's autonomy and expertise. The Estonian Defence League (Kaitseliit) and Lithuania's integration of the Riflemen's Union into national defense planning illustrate how historical volunteer defense organizations can be effectively modernized to address contemporary hybrid threats while maintaining their civilian character.

Third, significant challenges persist across all examined contexts. These include: resource constraints limiting civil society's operational capacity; variable levels of trust between state security institutions and civil society organizations; legal ambiguities regarding civil society's role during crises; and difficulties in maintaining appropriate boundaries between state and civil society in security matters.

Fourth, the research reveals that civil society's most distinctive contributions to national resilience lie in areas where traditional security institutions typically demonstrate limitations: community-level engagement, rapid response flexibility, specialized expertise (particularly in emerging domains like cybersecurity), trust-building with vulnerable populations, and transnational cooperation networks that operate beyond state constraints.

The insights provided by Rimvydas Adomavičius, one of the early leaders of Lithuania's Komendantūros system, reinforce the importance of structured civil-military integration for enhancing national resilience. His firsthand account confirms that successful civil society engagement in defense requires clear organizational structures, realistic training focused on specific wartime tasks, and approaches that respect the primarily civilian nature of participants' lives and careers. The Lithuanian experience demonstrates that defense structures can effectively incorporate civilian capabilities when they provide meaningful participation opportunities tailored to various commitment levels and when they emphasize the protection of participants' own communities, making abstract national defense concepts personally relevant.

To summarize, the findings indicate that successful civil-military cooperation models share common institutional elements such as legal mandates, structured training programs, and mutual respect between government and civil society. At the same time, notable differences in implementation, political context, and resource availability shape the effectiveness of these models.
In cases like Lithuania and Estonia, civil society has become a structured and strategic partner in defense. Georgia's trajectory, while promising, remains constrained by evolving political dynamics and institutional ambiguities. The contribution of civil society in each context depends not only on volunteerism but also on enabling environments that preserve CSO autonomy and pluralism.
Given the shared legacy of Soviet-era institutions and similar security challenges, the policy models and civil-military frameworks analyzed here may be adapted to strengthen resilience and preparedness in other Eastern European and NATO partner states.
While this study highlights promising practices, it also cautions against uncritical optimism. Whole-of-society approaches must be designed to avoid the risk of instrumentalizing civil society or compromising its independence in the name of national security.

*Reflection on the Transformative Role of Civil Society in Modern Security*
The findings of this research point to a fundamental transformation in how security is conceptualized and practiced in the face of hybrid threats. As warfare increasingly targets societal cohesion, information environments, and civilian infrastructure rather than military targets alone, the boundary between civilian and military domains has eroded. This transformation necessitates rethinking traditional security approaches that rely exclusively on state institutions.

Civil society's emerging role in national security represents not merely an expansion of existing security paradigms but a qualitative shift toward more distributed, adaptive, and socially embedded security practices. This shift aligns with the theoretical frameworks outlined at the outset—resilience theory, human security, and whole-of-society approaches – which emphasize security as a co-produced outcome emerging from the interactions of multiple actors across social systems.

The Baltic and Georgian experiences demonstrate that civil society can transform security practices in several critical ways. First, by localizing security – bringing defense concepts and practices into communities and everyday spaces where hybrid threats often manifest, but traditional security institutions rarely reach. Second, by democratizing security, expanding participation beyond professional security actors to include diverse citizen perspectives and capabilities. Third, by humanizing security, recentering defense efforts on the protection of human values, social cohesion, and democratic processes rather than territorial integrity alone.

This transformative potential is perhaps most evident in the Baltic cyber defense models, which have pioneered approaches to digital resilience that fundamentally rely on volunteer expertise and civil society networks rather than traditional military structures. Similarly, Lithuania's approach to societal resilience through the Riflemen's Union demonstrates how historical civil defense traditions can be reimagined to address contemporary hybrid threats.

Nevertheless, this transformation brings legitimate concerns regarding the militarization of civil society, the potential erosion of civilian oversight, and risks to the independence that makes civil society effective. Successful models, as seen in Estonia and increasingly in Lithuania, maintain clear distinctions between military and civilian domains while creating structured interfaces for collaboration. These balanced approaches preserve civil society's distinctive character while harnessing its complementary capabilities for national resilience.

*Call for Further Research and Cross-National Cooperation*

The evolving nature of both hybrid threats and civil society responses underscores the need for continued research and cross-national learning. Several promising directions for future investigation emerge from this study:

- **Longitudinal assessment of effectiveness:** Research tracking the long-term impact of civil society security initiatives on national resilience metrics would significantly advance understanding of which approaches yield sustainable results. This should include developing standardized metrics for evaluating civil society's contributions to security outcomes.
- **Public perception and legitimacy:** Further study is needed regarding how citizens perceive civil society's security role and how these perceptions influence the legitimacy and effectiveness of whole-of-society defense approaches. This is particularly important in contexts like Georgia, where historical experiences may complicate public trust in security institutions.
- **Knowledge transfer mechanisms:** Research examining how security knowledge and practices transfer between state institutions and civil society organizations – and across national contexts – would enhance understanding of effective capacity-building approaches.
- **Digital dimensions of civil resilience:** The role of digital platforms, social media, and online communities in both amplifying vulnerabilities and

enabling civil society responses to hybrid threats represents a critical frontier for security research.

- **Ethical frameworks:** Developing robust ethical guidelines for civil-military cooperation that protect civil society's independence while enabling effective security partnerships remains an urgent research need.

Beyond research, this study underscores the value of cross-national cooperation platforms where civil society organizations, security practitioners, and policymakers can exchange experiences and best practices. The Baltic-Georgian context examined here represents a microcosm of wider challenges facing democracies globally. Establishing formal mechanisms for knowledge sharing, particularly between countries with advanced civil society security integration and those developing such approaches, could accelerate the dissemination of effective models.

In conclusion, as modern security threats increasingly target the societal fabric rather than conventional military objectives, civil society's role in national resilience will only grow in importance. The experiences examined in this study suggest that effective national preparedness increasingly depends not on the strength of military capabilities alone, but on the adaptive capacity of whole societies, with civil society organizations serving as critical connective tissue between citizens, communities, and formal security institutions. This evolution toward more inclusive security paradigms may ultimately prove the most effective response to the hybrid threats characterizing our contemporary security landscape.

***Disclaimer***

The views represented in this paper are those of the author and do not reflect the official policy or position of the Government of Georgia and Sulkhan-Saba Orbeliani University.

***Conflict of Interest Statement***

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

***Declaration on the Use of AI Too***ls

The author utilized OpenAI's ChatGPT and Anthropic's Claude to assist with language editing during the drafting of this manuscript. The author retains full responsibility for the content, analysis, and accuracy of the work.

## References

**Adomavičius, Rimvydas.** 2025. *Written interview on the leadership of Lithuania's Komendantūros system.* Personal communication.

**Aisi.** n.d. *Mission and history.* https://aisi.org.ge/ .

**Boin, Arjen, and Martin Lodge.** 2016. "Designing resilient institutions for transboundary crisis management: a time for public administration ." *Special Issue: Symposium: Designing Resilient Institutions for Transboundary Crisis Management* 94 (2). https://doi.org/10.1111/padm.12264.

**Edwards, Michael.** 2014. *Civil Society.* Cambridge: Polity Press.

**Estonian Defence League.** n.d. *Kaitseliit.* https://www.kaitseliit.ee/en/edl.

**European Commission.** 2016. "JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Joint Framework on countering hybrid threats a European Union response." Brussels. https://tinyurl.com/mwubyt2s.

**European Parliament.** 2024. *European Parliament resolution of 25 April 2024 on attempts to reintroduce a foreign agent law in Georgia and its restrictions on civil society.* https://www.europarl.europa.eu/doceo/document/TA-9-2024-0381_EN.html.

**Freedom House.** 2025. *Georgia.* https://freedomhouse.org/country/georgia/freedom-world/2025.

**Hoffman, Frank G.** 2007. "Conflict in the 21st Century: The Rise of Hybrid Wars." *Potomac Institute for Policy Studies.* https://tinyurl.com/mb53ct5t.

**Jungwirth, Rainer, Hanna Smith, Etienne Willkomm, Jukka Savolainen, Marina Alonso Villota, Maxime Lebrun, Aleksi Aho, and Georgios Giannopoulos.** 2023. "Hybrid Threats: A Comprehensive Resilience Ecosystem." Publications Office of the European Union, Luxembourg. doi:10.2760/37899.

**Kaska, Kadri, Anna-Maria Osula, and LTC Jan Stinissen.** 2023. *The Cyber Defence Unit of the Estonian Defence League. Legal, Policy and Organisational Analysis.* Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/CDU_Analysis.pdf.

**Lithuanian Armed Forces.** n.d. *The Military Commandant's Board is conducting exercises in Klaipėda for the first time.* https://www.kariuomene.lt/kas-mes-esame/naujienos/karo-komendanturos-valdyba-pirma-karta-vykdo-pratybas-klaipedos-mieste/26478.

**Lithuanian Riflemen's Union.** n.d. *About the Lithuanian Riflemen's Union.* https://www.sauliusajunga.lt/en-puslapis/.

**Loada, Augustin, and Ornella Moderan.** 2015. "Civil Society Involvement in Security Sector Reform and Governance." In *Toolkit for Security Sector Reform and Governance in West Africa*. Geneva: DCAF. https://www.dcaf.ch/sites/default/files/publications/documents/ECOWAS_Toolkit_T6_EN.pdf.

**LRT.** 2024. *Lithuania sets up wartime civilian force – explainer.* https://tinyurl.com/473a5ez8.

___. 2022. *Lithuanian parliament expands activities of Riflemen's Union.* https://tinyurl.com/46m44a9d.

**Mazniashvili Legion.** n.d. *About us.* https://legionerebi.com/.

**MoD, Ministry of Defence Republic of Latvia.** n.d. *Cooperation with NGOs.* https://www.mod.gov.lv/en/nozares-politika/public-involvement/cooperation-ngos.

**NATO.** 2024. *Resilience, civil preparedness and Article 3.* https://www.nato.int/cps/en/natohq/topics_132722.htm.

**Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum.** 2008. "Community Resilience as a Metaphor, Theory, Set of Capacities, and Strategy for Disaster Readiness." *American Journal of Community Psychology* 41 (1-2): 127-150. doi:10.1007/s10464-007-9156-6.

**Parliament of Georgia.** 2023. "Defense Code of Georgia." Law of Georgia.

**Perry, Ronald W., and Michael K. Lindell.** 2003. "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process." *Disasters* 27 (4): 336-350. doi:10.1111/j.0361-3666.2003.00237.x.

**Republic of Lithuania.** 1997. "Law on the Lithuanian Riflemen's Union, No. VIII-397."

**Riigikogu.** 2013. *The Estonian Defence League Act.* https://www.riigiteataja.ee/en/eli/521032014005/consolide.

**Salamon, Lester M.** 1994. "The Rise of the Nonprofit Sector." *Foreign Affairs* 73 (4): 109–122. https://doi.org/10.2307/20046747.

**Salamon, Lester M., and Helmut K. Anheier.** 1997. *Defining the Nonprofit Sector: A Cross-national Analysis.* Manchester University Press.

**Sedra, Mark.** 2022. *A People-Centered Approach to Security.* New York, USA : One United Nations Plaza. https://www.undp.org/publications/people-centered-approach-security.

**Walker, Brian, C.S. Holling, Stephen R. Carpenter, and Ann Kinzig.** 2004. "Resilience, adaptability and transformability in social–ecological systems." *Ecology and Society* 9 (2): art. 5. http://www.ecologyandsociety.org/vol9/iss2/art5/.

## **Appendix A:** Comparative Analysis of Civil Society Role in National Security Across Baltic States and Georgia

| Key Element | Lithuania | Latvia | Estonia | Georgia |
|---|---|---|---|---|
| **Primary Civil Society Organizations** | - Lithuanian Riflemen's Union (LRU)<br>- Komendantūros (wartime civilian forces) | - Zemessardze (National Guard)<br>- Military/veterans associations<br>- Research/policy organizations<br>- Historical memory organizations | - Estonian Defence League (Kaitseliit)<br>- Women's Voluntary Defence Organization (Naiskodukaitse)<br>- Youth Organizations (Kodutütred & Noored Kotkad)<br>- Cyber Defence Unit | - Mazniashvili Legion<br>- Aisi |
| **Legal Framework** | - Law on the Lithuanian Riflemen's Union<br>- 2024 Regulatory Framework for Komendantūros | - Formal partnership frameworks with MoD<br>- Delegation agreements with CSOs | - Estonian Defence League Act<br>- Legal person governed by public law | - 2023 Defense Code of Georgia<br>- Chapter XVII on "volunteering in the defense sector" |
| **Membership Size** | - LRU: ~15,000 members (target: 50,000)<br>- Komendantūros: target 10,000 citizens | - Multiple organizations with varied membership | - ~18,000 direct members<br>- ~29,000 total volunteers with affiliated organizations | - Mazniashvili Legion: ~1,600 members<br>- Aisi: trained over 1,000 volunteers |
| **Governance Model** | - LRU subordinated to government rather than defense minister<br>- Advisory council for coordination | - Ministry of Defence maintains formalized partnerships with various NGOs | - Military principles while relying on "free will and self-initiative"<br>- 16 districts corresponding to county boundaries | - LEPL "Volunteer" under Ministry of Defense oversight<br>- Requires Ministry approval for volunteer organization status |
| **Unique Innovations** | - "Society-wide defense" approach<br>- Clear distinctions between armed ("kinetic") and non-armed ("non-kinetic") roles | - Systematic integration of historical commemoration into resilience strategy<br>- International networking for CSOs | - Cyber Defence Unit leveraging civilian IT expertise<br>- Comprehensive affiliated organizations structure including women and youth | - Recently formalized total defense approach<br>- New legal entity specifically for coordinating volunteer activities |
| **Training Focus** | - Structured citizenship and defense skills courses<br>- Dedicated training center for riflemen | - Patriotic educational events<br>- Intergenerational knowledge transfer | - Systematic tiered training (basic, professional, refresher, instructor preparation)<br>- Specialized cyber defense training | - Military-camping courses<br>- Training in topography, first aid, trench preparation, forest camping, etc. |
| **Key Challenges** | - Integration of volunteer capabilities into formal defense planning | - Ensuring sustainable funding for CSO activities<br>- Balancing state guidance and CSO independence | - Maintaining balance between military functionality and civic voluntarism | - Evolving state-civil society relations<br>- Legal ambiguity<br>- Financial burden of liability requirements |
| **Strategic Approach** | - Lessons drawn from Ukraine's experience<br>- "Very clear algorithm" for incorporating civilian capabilities into military planning | - Structured international partnerships<br>- Strategic use of veterans' organizations for continuity | - Distributed territorial approach ensuring nationwide coverage<br>- Digital society integration with traditional defense | - Total defense approach still in early implementation<br>- Volunteer registry as "internal information" of the Ministry |

## **Appendix B:** Written interview on leadership of Lithuania's Komendantūros system

### INTERVIEW QUESTIONS

**1. Establishment and Evolution**: As one of the early leaders of the Komendantūros system, could you describe the initial vision behind its establishment in 2024 and how the organization has evolved since then? What were the key challenges you faced during the implementation phase?

**2. Civil-Military Integration**: The Komendantūros represents an innovative approach to incorporating civilian capabilities into national defense. How would you characterize the relationship between these wartime civilian forces and traditional military structures? What mechanisms proved most effective in facilitating cooperation?

**3. Volunteer Motivation and Retention**: What strategies did you employ to attract and retain the civilian participants? How did you address the challenge of maintaining volunteer engagement during peacetime when the organization's wartime purpose might seem less immediate?

**4. Training Methodology**: Could you elaborate on the training approach developed for Komendantūros members? How did you balance the need for military-relevant skills with the reality that participants maintain primary civilian careers and can only dedicate limited time to training?

**5. Lessons for Other Countries**: Based on your experience leading the Komendantūros, what recommendations would you offer to other countries, particularly those like Georgia that are in earlier stages of developing civil society integration into defense structures? What elements of the Lithuanian model do you believe are most transferable to other contexts?

### ANSWERS

❶ The establishment of the Komendantūros system in 2024 emerged from our need to strengthen Lithuania's total defense posture through better civil-military integration. Our initial vision was to create a structure that would serve dual purposes: ensuring effective mobilization in crisis and providing rear security operations if needed.

Lessons from Ukraine's experience were instrumental in shaping our approach. The war in Ukraine demonstrated clearly that effective territorial defense requires not only frontline military capabilities, but also robust rear-area security, protection of critical

infrastructure, and mobilization systems that can rapidly integrate civilian resources into the defense effort. We observed how Ukrainian cities and towns that established effective civil-military coordination were better able to resist and recover from attacks, evacuate civilians, and maintain essential services even under extreme pressure.

The foundation of our approach was reorganizing and merging the Military Commandant's Offices with the Military Conscription and Recruitment Service. This allowed us to create a coherent system where commandant's offices could function effectively both in peacetime and wartime.

The key challenges we faced during implementation included:
First, establishing clear lines of authority and coordination between military and civilian structures. We needed to ensure that municipal administrations and commandant's offices could work together seamlessly on mobilization plans and facility protection. Ukraine's experience showed that unclear chains of command between military and civilian authorities could lead to dangerous gaps in emergency response.

Second, attracting sufficient numbers of patriotic citizens willing to commit to defense preparations while maintaining their civilian lives and careers. We initially aimed for 2-5 thousand volunteers, and by March 2025, we had approximately 2.5 thousand citizens actively joining commandants, with 250 having completed the Basic Commandant Unit Soldier Course. The Ukrainian volunteer mobilization demonstrated both the potential and challenges of integrating civilian volunteers into defense structures during crisis.

Third, securing adequate resources for training and equipment. Each commandant's unit required approximately 12 thousand euros for new equipment alone, multiplied across the country's municipalities. Ukraine's experience underscored that even basic equipment can make a significant difference in effectiveness when properly distributed and utilized.

The system evolved from concept to reality through a regional structure consisting of a headquarters and 6 regional military commandants in Vilnius, Kaunas, Klaipėda, Šiauliai, Panevėžys, and Alytus, each responsible for their city and district municipalities. This territorial approach was directly informed by Ukraine's experience with local defense councils and territorial defense units that proved most effective when aligned with existing administrative boundaries.

❷ The relationship between our wartime civilian forces and traditional military structures is best characterized as complementary, with clear delineation of responsibilities. The Komendantūros represents the military in municipalities while simultaneously serving as the conduit through which civilian capabilities and resources can be integrated into defense planning.

The most effective mechanisms for facilitating cooperation included:
First, establishing a clear organizational structure where regional commandants oversee municipal commandants, creating a chain of command that parallels civilian administrative divisions. This territorial alignment made coordination with local governments more intuitive.

Second, joint planning processes with municipal administrations for mobilization, protection of important facilities, and other contingency plans. These collaborative efforts forced both military and civilian authorities to understand each other's capabilities and constraints.

Third, involving the Lithuanian Riflemen's Union as a bridging organization between purely civilian volunteers and military personnel. The Riflemen brought both paramilitary capabilities and civilian connections that proved invaluable.

Finally, our regular training exercises involving both military personnel and civilian volunteers created shared experiences and mutual understanding that proved essential for building trust between the different components of our total defense approach.

❸ To attract and retain civilian participants, we employed several effective strategies:
First, we appealed to patriotism and civic duty. Our public messaging emphasized that the Komendantūros provides a concrete way for citizens to contribute to national defense without necessarily joining the professional military or volunteer forces. A public survey commissioned by the Ministry of National Defense confirmed that more than half (52 percent) of the country's citizens would be willing to contribute to armed resistance during aggression against Lithuania.

Second, we created a tiered approach to involvement, allowing citizens to participate according to their capabilities, time availability, and commitment level. This flexibility was crucial for attracting professionals who couldn't commit to more intensive military service.

Third, we provided meaningful training that developed not only military skills, but also emergency management capabilities useful in civilian contexts. This dual-use approach to skills development made the training more immediately relevant.

To maintain engagement during peacetime, we:

- Organized regular training events (3-10 days per year) that created a sense of community and purpose
- Integrated commandant units with the National Defense Volunteer Forces for training, exposing our members to professional military standards
- Emphasized the protection of their own communities and important local facilities, making the commitment personal and concrete
- Created pathways for advancement and recognition within the system.

❹ Our training approach for Komendantūros members was designed around several core principles:
First, we developed a Basic Commandant Unit Soldier Course that provided essential military knowledge and skills in a condensed format. This became our standardized initial training program, with 250 citizens completing it by early 2025 and plans for 1,000 more by the end of the year.

Second, we leveraged the expertise of the National Defense Volunteer Forces to deliver training, ensuring professional military standards while recognizing the part-time nature of our volunteers' commitment.

Third, we focused training on specific wartime tasks related to rear security, protection of important facilities, and support to mobilization rather than attempting to create fully combat-ready units. This mission-specific approach allowed for more efficient use of limited training time.

To balance military skills development with civilian career demands, we:

- Limited annual training requirements to 3-10 days per year
- Scheduled training to coincide with exercises involving other reserve components
- Tailored assignments based on individuals' civilian skills and qualifications
- Created a progressive training system that built competencies over time rather than requiring intensive initial training

We also established more accessible health and physical requirements compared to regular military service, opening participation to a broader segment of society who might otherwise be unable to contribute to defense efforts.

❺ Based on our experience with the Komendantūros, I would offer several recommendations to countries developing similar civil society integration into defense structures:
First, build on existing institutions rather than creating entirely new ones. Our success partly stemmed from merging and reorganizing the Military Commandant's Offices with the Military Conscription and Recruitment Service, which provided an institutional foundation and credibility.

Second, create clear territorial alignment between military and civilian administrative structures. Our regional and municipal commandant system parallels civilian governance, facilitating coordination and local ownership.

Third, develop flexible participation models that accommodate varying levels of citizen commitment. Not everyone can or should contribute in the same way, but creating diverse pathways to participation maximizes societal involvement.

Fourth, focus on realistic wartime tasks that civilians can perform with limited training. Protecting local infrastructure, supporting mobilization, and facilitating civil-military coordination are more appropriate than frontline combat roles.

Fifth, leverage public patriotism and willingness to contribute. Our survey showed that 52 percent of citizens would contribute to armed resistance and 61 percent to peaceful resistance. This latent willingness needs practical channels for expression.

The most transferable elements of the Lithuanian model include:

- The regional commandant structure that bridges national military and local civilian authorities
- The incorporation of existing civil society organizations (like our Riflemen's Union)
- The dual peacetime/wartime function of commandant's offices
- The focus on local defense and protection of familiar territory and facilities
- The graduated training system that builds capabilities over time

For Georgia specifically, I would emphasize the importance of creating a system that respects local traditions and existing civil-military relationships while providing a structured framework for civilian contributions to national resilience.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Between Authority and Resistance: the Political Evolution of Gaza from 1948 to Hamas

**Bachelor finalist, Mariana RODRIGUES***
**Lt.Col. Cav Pedro FERREIRA, PhD****
*University of Lisbon
e-mail: mrodrigues21@edu.ulisboa.pt
**Portuguese Military Academy Research Centre
e-mail: ferreira.pna@exercito.pt

## Abstract

This paper examines the historic and political dynamics of administration in Gaza, focusing on the impact of Egyptian rule, Palestinian administration, and the rise of Hamas. The relevance of this topic lies in its implications for understanding the Palestinian struggle for self-determination. The aim is to analyze how the different government structures have shaped Palestinian identity and resistance. A qualitative approach was used, focusing on historical analysis and contextual examination of key events, based on a review of academic articles and books. The findings reveal that the Egyptian administration laid the foundations for political organisation, the Oslo Accords introduced complexities that fueled internal divisions, and the emergence of Hamas further transformed the socio-political landscape, intertwining the administration with armed resistance. This work contributes to a deeper understanding of the interaction between the administration and the resistance in Gaza.

**Keywords:**
administration; Hamas; identity; Palestine; resistance.

**Article info**
Received: 15 May 2025; Revised: 6 June 2025; Accepted: 13 June 2025; Available online: 27 June 2025

Citation: Rodrigues, M., and P. Ferreira. 2025. "Between Authority and Resistance: the Political Evolution of Gaza from 1948 to Hamas." *Bulletin of "Carol I" National Defence University*, 14(2): 200-214. https://doi.org/10.53477/2284-9378-25-23

Since the 20th century, the Gaza Strip has been one of the most unstable and disputed territories in the Middle East, marked by successive forms of domination and resistance. After the collapse of the Ottoman Empire and the British Mandate in Palestine, Gaza was administered by Egypt (1948-1967), before passing to Israeli control after the Six-Day War. More recently, it has undergone profound political transformations, including a brief control by the Palestinian Authority since 2007, governance by Hamas, in a context of international isolation and military blockade. The relevance of this study lies in the analysis of a key moment in this trajectory: the First Intifada (1987-1993), understood as a massive and organized expression of civil resistance to the Israeli occupation and as a turning point in the consolidation of Palestinian national identity.

The subject of administration in Gaza, particularly under Egyptian rule, Palestinian control, and the subsequent rise of Hamas, are of significant importance in understanding the complex socio-political landscape of the region. This article investigates the historic and contemporary dynamics of governments in Gaza, addressing the critical problem of how these different forms of control have shaped the lives of the Palestinian people and influenced the wider Israeli-Palestinian conflict. The importance of this research lies in its potential to illuminate the factors contributing to ongoing tensions and the quest for Palestinian self-determination.

The problem we aim to investigate centers on understanding the main socio-political factors that led to the outbreak of the First Intifada and the way this movement influenced the construction and affirmation of Palestinian collective identity. This question is crucial, as it allows an in-depth reading of the internal dynamics of Palestinian society under occupation, the resistance strategies adopted, and their symbolic and political effects, both locally and internationally. At the same time, it aims to analyze how the forms of governance - from Egyptian rule to the current Hamas administration - shaped the context that led to the Intifada and its subsequent developments.

This article adopts a qualitative and historical-analytical approach, based on a critical review of the literature and an analysis of secondary sources. This method is particularly suitable as it allows for a comprehensive understanding of the historical processes and political structures that influence governance and resistance in Gaza.

The article is organized chronologically, starting with the period of Egyptian rule (1948-1967), passing through Israeli control and the establishment of the Palestinian Authority in the 1990s, and culminating with the rise of Hamas and the current governance in Gaza. It will also analyze the context and causes of the First Intifada and discuss its impact on the construction of Palestinian identity. The main aim of the research is to analyze how the different forms of administration in Gaza – including Egyptian rule, Palestinian governance, and Hamas control – have shaped the socio-

political landscape of the region and influenced the Palestinian people's struggle for self-determination. The research question guiding this study is: "How have Egyptian rule, Palestinian control, and Hamas governance shaped the socio-political landscape of Gaza and influenced the Palestinian struggle for self-determination?"

## Egyptian domination

In the 1960s, the Gaza Strip was under Egyptian administration, and the rest of Palestinian territory was divided. In June 1967, the Six-Day War took place between Israel and a coalition of Arab states led by Egypt, including Syria and Jordan, with Iraq and Lebanon playing minor roles. In the Arab world, the war is known as the June War or al-Naksa, which means setback or calamity. The period between 1949 and June 1967 was characterized by a series of military confrontations between Israel and these countries that preceded the Six-Day War (Haun 2023).

The Suez Crisis of 1956 was an important milestone in the escalation of tensions that would lead to the Six-Day War in 1967. During the crisis, Israel temporarily occupied Sinai, claiming self-defense against Fedayeen attacks from the Gaza Strip, then under Egyptian control, and aiming to reopen the Straits of Tiran, blocked to Israeli shipping. Under international pressure, especially from the US, Israel withdrew, and the UN established an emergency force (UNEF) in Sinai. In May 1967, Egypt demanded the withdrawal of UNEF, blocked the Straits of Tiran again, and mobilized its troops in Sinai, measures considered by Israel to be acts of war. The defence treaty between Egypt and Jordan and statements by Arab leaders increased the sense of existential threat in Israel, leading to the outbreak of the Six-Day War (Sabel 2022, 47).

As early as May 1967, the Soviet Union passed on fabricated information to Syria and Egypt about an alleged mobilization of Israeli forces on the Syrian border. In response to this information, Egypt mobilized troops in Sinai on 14 May, requested the withdrawal of the United Nations Emergency Force (UNEF) on 16 May and declared the closure of the Straits of Tiran to Israeli shipping on 22 May, which was marked as the immediate cause of the war (Goldstein 2018).

On 5 June 1967, Israel launched Operation Moked ("focus" in Hebrew), a pre-emptive air strike that destroyed a large part of the Egyptian air force on the ground, gaining air supremacy. Later that day, the Israeli Air Force (IAF) turned its attention to the Syrian and Jordanian air forces, quickly gaining air superiority over the West Bank and the Golan Heights. Without the threat of enemy air strikes, the Israeli army began a three-pronged offensive in Sinai, which resulted in the collapse of the Egyptian army the following morning. In the course of a week, Israel secured its borders and doubled its territory, conquering the Sinai, the Old City of Jerusalem, the West Bank, and the Golan Heights. A UN Security Council ceasefire was observed

on 10 June 1967 (Haun 2023).
Although it was a decisive victory for Israel, the Six-Day War did not result in a peace agreement. In turn, a series of cross-border air and artillery attacks began a low-intensity war of attrition, which continued for the next three years (Haun 2023). Some consider this war to be a direct continuation of the 1948 War (Martinelli 2022, 154).

This war had consequences such as a new wave of Palestinian refugees, estimated at around 200,000 people, who joined those already displaced by the 1948 war, led to the Israeli military occupation of the West Bank, East Jerusalem, the Gaza Strip, the Sinai Peninsula and the Golan Heights, and is seen as a significant defeat for Arab nationalism. In November 1967, the UN Security Council passed Resolution 242, which called for an Israeli withdrawal from the occupied territories and a just solution to the refugee problem (Martinelli 2022, 136-138, 153-155, 162-166, 238).
Some argue that the war was the result of a miscalculation by the Egyptian leadership. Others suggest that there was subtle coordination, but not a military conspiracy, between Israel and the United States, while the Soviet Union and Syria may have incited Egyptian involvement in the crisis (Yossef 2006).

The war had a significant impact on Palestinian national identity and the rise of armed resistance, with the decline of pan-Arabism and the rise of political Islam within the Palestinian movement. Following Egypt's defeat, Israel occupied Gaza, which until then had been under Egyptian administration. The occupation marked the beginning of a new period of Israeli military control over the territory, drastically altering the political, social, and economic life of the region. Thousands of Palestinians were displaced, and there was a significant increase in repression and tensions between the local population and the occupying forces. Israel's continued presence in Gaza fueled Palestinian resentment and resistance, contributing to the emergence of movements like Hamas in the following decades and consolidating Gaza as one of the central focuses of the Israeli-Palestinian conflict (Martinelli 2022, 153).

## Israeli Occupation

Between the Six Day War (1967) and the First Intifada (1987), the Gaza Strip experienced two decades under Israeli military occupation, marked by repression, demographic growth, and growing Palestinian frustration. During this period, Israel built settlements in the region and imposed strict control measures, while the Palestinian population faced mobility restrictions, economic hardship, and a lack of civil rights (Sprague 2013). Egypt, despite having lost direct control over Gaza, continued to have symbolic influence, and the Palestinian cause remained alive throughout the Arab world. The lack of a political solution and worsening living conditions led to a build-up of tensions that would eventually explode in 1987 with the outbreak of the First Intifada, a popular uprising against the Israeli occupation that began in Gaza before spreading to the West Bank (Martinelli 2022, 154).

The First Intifada was then a period of widespread Palestinian civil unrest and resistance against Israeli occupation and policies that took place between 1987 and 1993, motivated by decades of frustration with military occupation, settlement expansion, and political stagnation. What many cite as the trigger for the First Intifada was an accident in Gaza that killed four Palestinians. After this accident, the movement quickly spread, taking the form of a widespread uprising with protests, strikes, boycotts, and clashes - symbolized by the "sons of stones" facing tanks with stones (Sotirović 2024). The resistance combined non-violent and violent actions, organized by a local leadership, the LNUL, which later aligned itself with the PLO (Palestine Liberation Organisation) (Farraj 2017). The Israeli response was marked by strong repression, with thousands of arrests and deaths. The Intifada strengthened Palestinian national identity, attracted international attention to the conflict, and prepared the ground for the Palestinian Declaration of Independence (1988) and the start of the Oslo Accords peace process (Naser-Najjab 2020).

The Gaza Strip was one of the main centers of the First Intifada and was the scene of intense clashes between Palestinians and Israeli forces. Popular resistance in Gaza was marked by protests, strikes, boycotts, and, above all, violent clashes, with young people throwing stones at Israeli forces. The Israeli military response was severe, including mass arrests, reprisals, and the use of excessive force, resulting in a large number of Palestinian deaths and injuries, especially among young people (Bjur 2014). In addition to physical repression, the Intifada had a major social and economic impact on Gaza. The blockade and restrictions increased, exacerbating economic difficulties, while violence and social instability further weakened community life. However, the Intifada also strengthened Palestinian identity in Gaza, consolidating the sense of resistance and the quest for an independent state (Junka 2006).

## Palestinian control

In order for there to be peace between Israel and the Palestine Liberation Organisation (PLO), the two parties agreed in 1993 to sign a series of agreements called the Oslo Accords. Signed by Yasser Arafat and Yitzhak Rabin in September 1993, the Oslo Accords, whose official name was the Declaration of Principles on Interim Self-Government Arrangements, or Declaration of Principles (DOP), provided for the establishment of a Palestinian National Authority in parts of the West Bank and Gaza Strip and the withdrawal of Israeli troops from Palestinian population centers (Bjur 2014). However, although the Accords were greeted with much acclaim by many, this was not well received by others, as settlement construction continued apace (Feldman 2008, 237).

After the Oslo Accords, the West Bank and Gaza were divided into three areas: Area A (approximately 65 per cent of Gaza and 3 per cent of the West Bank), where the

Palestinians had both security and civilian control; Area B (about 23 per cent of the West Bank), where the Palestinians controlled the civilian part and the Israelis maintained military control; and Area C, where Israel had total control. In the following years, a power station was built in Gaza, but it was destroyed by Israeli forces in the summer of 2006 (Feldman 2008, 294).

The Oslo process, which began in December 1992 and culminated with the signing ceremonies of 13 September 1993 on the White House lawn, was made up of a series of agreements designed to address a series of increasingly complex issues in an incremental way. The 1993 Declaration of Principles was followed in 1995 by the Taba or Oslo II Agreement, the 1998 Wye River Memorandum, and the 1999 Sharm el-Sheikh Memorandum. The PLO, for its part, concentrated on bringing the agreement into line internally with UN resolutions 242 and 338. Internationally, it appealed for assistance from the US and other members of the international community to ensure the implementation of the Accords. Unlike other peace processes, there was no significant external force capable of defining the terms of the debate or credibly guaranteeing that all parties would comply with the Oslo agreement. The gradual nature of the Oslo Accords also made them more susceptible to implementation failures, increasing the risk of internal opponents hindering their realization. Despite initial hopes that the Oslo Accords could lead to an end to the conflict, the Second Intifada began just over seven years later, plunging the region back into violence and dashing hopes for peace, which raised many questions about the failure of the Oslo process (Hancock and Weiss 2011).

These Accords resulted from the PLO's new approach to negotiating with the Israeli occupation, leading to Israeli recognition of the PLO as the representative of its people and the establishment of the Palestinian National Authority (PNA). However, these agreements were subsequently highly criticized and eroded the legitimacy of the PLO in many sectors of Palestinian society. The Oslo Accords were intended, among other things, not to suffer another intifada, which eventually happened, and for the PNA to be a complementary control police for its more revolutionary population (Martinelli 2022, 194).

The expansion of settlements in the West Bank and East Jerusalem, the construction of the Separation Wall, the isolation of Gaza, the split between Fatah and Hamas, and Arab representation within Israel all contributed to discrediting the peace process. These factors created significant obstacles to the implementation of the Oslo Accords and increased mistrust between the parties involved in the peace process. After the Second Intifada, some Palestinians advocated a single state as a solution (Martinelli 2022, 299).

In the context of the Oslo I Accords, Palestinian political alliances were formed, such as the alliance between Fatah and the PPP, known as Jerusalem and State, and the alliance between Islamists and the PFLP-DFLP, called Jerusalem First, which rejected

Oslo I's "Gaza and Jericho first" plan. After Oslo I, the first Palestinian National Security Forces (PNSF) were mobilized in Jericho and Gaza. The borders of Area A, defined by Oslo II in 1995, were demarcated with concrete blocks, with numerous Israeli and Palestinian checkpoints (Farraj 2019).

The Oslo Accords do not refer to the possibility of creating a Palestinian state and leave open the question of the final status of the West Bank and Gaza. According to the Oslo Accords, the Palestinian Authority received 'all civil powers and responsibilities' in the areas of the West Bank with an Arab population. However, the interim agreement stipulated that the Palestinian Authority would have no powers in foreign affairs (Sabel 2022, 270, 392) .

After the Oslo Accords, there was also the Peace Treaty between Israel and Jordan, signed in 1994, which had some impact on the Gaza Strip. Although the treaty was not directly involved, it represented a significant change in the regional context of the Israeli-Palestinian conflict. By normalizing relations with Israel, Jordan weakened the United Arab Front against Israel and left the Palestinians, including those in Gaza, more politically isolated (Sabel 2022, 236, 300) .

For many Palestinians, especially in Gaza, the treaty was viewed with suspicion and even as a betrayal of the Palestinian cause, as it was signed before the creation of a Palestinian state. It also symbolized the growing alignment of some Arab countries with Israel without the Palestinian question being resolved. In return, the treaty strengthened Israel's security on its eastern borders, allowing Tel Aviv to concentrate more resources on managing and repressing the occupied territories, including Gaza (Martinelli 2022, 111, 113, 125) .

In 1994, Israel withdrew from parts of the Gaza Strip, and Yasser Arafat came to govern the region on behalf of the PNA. The continued construction of Israeli settlements, restrictions on mobility, economic blockades, and the perception that Israel was not fully honoring its commitments undermined the confidence of the Palestinian population. In Gaza, the economic situation deteriorated with high levels of unemployment and poverty, aggravating popular frustration (Bjur 2014).

Discontent grew further with perceived corruption in the PNA leadership and internal repression. During this period, Islamist groups such as Hamas gained strength in Gaza, criticizing the Oslo Accords and rejecting coexistence with Israel. Rising tensions, coupled with the stagnation of the peace process and sporadic clashes with Israeli forces, culminated in the outbreak of the Second Intifada in September 2000, following Ariel Sharon's provocative visit to the Al-Aqsa Mosque compound in Jerusalem (Naser-Najjab 2020).

The Camp David negotiations, held in July 2000, were an attempt to reach a final agreement between Israel and Palestine, mediated by the United States and led

by President Bill Clinton, with the participation of Israeli Prime Minister Ehud Barak and Palestinian leader Yasser Arafat. The negotiations addressed key issues such as borders, security, the status of Jerusalem, Israeli settlements, and the right of return of Palestinian refugees. These complex and sensitive issues were central to the negotiations, reflecting the main points of contention between the parties involved. Despite progress on some points, the negotiations broke down mainly due to disagreements over Jerusalem and the refugees (Freas 2017) . Israel proposed concessions that included part of East Jerusalem, but Arafat considered the offer insufficient and feared losing legitimacy with his people. The failure of the negotiations contributed to rising tensions that culminated in the outbreak of the Second Intifada a few months later (Salihu 2024).

The Second Intifada, also known as the Al-Aqsa Intifada, was a remarkable period of violence in the context of the Israeli-Palestinian conflict, which took place from September 2000 to January 2005. This period was characterized by intense clashes, suicide attacks, and military operations, resulting in a great loss of life and further aggravating tensions between Israelis and Palestinians. Unlike the First Intifada, which was predominantly non-violent, the Second Intifada was characterized by intense violence (Asali, Abu-Qarn and Beenstock 2024).

Some authors suggest that Yasser Arafat premeditated the Intifada after his return from the Camp David Accords (Naser-Najjab 2020). Palestinian frustration with the stalled peace process and the failure to resolve the final status issues of refugees, settlements, and Jerusalem also contributed to the climate of tension (Abu-Nimer 2002).

The Second Intifada was marked by armed attacks and suicide bombings perpetrated by Palestinian militants. In response, the Israeli army reoccupied Palestinian towns and refugee camps and engaged in clashes with Palestinian militants and security forces. The level of violence from both was high, resulting in the deaths of 3243 Palestinians and 957 Israelis, as well as thousands of injuries (Asali, Abu-Qarn and Beenstock 2024).

Hamas, the Islamic Resistance Movement, played a central role in the Second Intifada, being the main advocate of suicide bombers. Other Palestinian factions also took part in the violence, including the Fatah-affiliated Al-Aqsa Martyrs' Brigades and Islamic Jihad (Rojas and Matta 2016). Hamas abandoned suicide attacks around 2005, which coincided with an increase in the internal Palestinian conflict and preparations for the 2006 legislative elections.

The Second Intifada led to increased polarization and a further deterioration in relations. There was a rise in Islamist militancy and a crisis in the Palestinian national movement (Junka 2006). After the Second Intifada, some Palestinians began to advocate a one-state solution. Interestingly, the co-operation between Israelis and Palestinians that took place during this period had a pacifying effect, suggesting that the Intifada could have been

even more violent and prolonged without it (Asali, Abu-Qarn and Beenstock 2024). The Second Intifada represented a significant increase in violence in the Israeli-Palestinian conflict, with serious consequences for both sides and the prospects of peace (Abu-Nimer 2002).

Gaza became one of the main stages of the conflict, suffering from intense Israeli military operations, blockades, and the increasing militarization of Palestinian factions, especially Hamas (Abu-Amr 1993). The generalized violence, which included suicide attacks, bombings, invasions, and demolitions, caused thousands of deaths and injuries, largely civilians (Robinson 2004).

Gaza's economy collapsed due to the siege, the destruction of infrastructure, and the closure of borders, exacerbating (Hroub 2006) poverty and unemployment. The atmosphere of war and repression reinforced popular support for armed groups and Hamas, which strengthened politically during the conflict and ended up winning the 2006 legislative elections. The Second Intifada also contributed to the weakening of the Palestinian Authority in Gaza, culminating in Israel's unilateral withdrawal from the Strip in 2005 and, later, the political split between Fatah (West Bank) and Hamas (Gaza). This division hinders a unified Palestinian front, weakening diplomatic efforts for an independent Palestinian state (Abu-Amr 1993).

## The rise of Hamas

The Gaza Strip came under Hamas control in 2007 after clashes with Fatah. Hamas (Harakat al-Muqawama al-Islamiyya), which means "zeal" in Arabic and is the acronym for the Islamic Resistance Movement, emerged during the First Intifada, marking a period of political revitalization for Islamic forces in the West Bank and Gaza Strip in the face of Israeli occupation and secular forces led by the PLO. Hamas was born from within the Muslim Brotherhood in Palestine, with the aim of actively participating in the resistance against the Israeli occupation. Its creation was partly a response to the initial attitude of the Muslim Brotherhood, which had distanced itself from active resistance (Abu-Amr 1993).

The charter of 18 August 1988 defines Hamas' philosophy, logic, and positions. In this charter, Hamas considers all of Palestine to be Muslim land ('waqf') that cannot be ceded. The stated aim of the charter is the destruction of the State of Israel and the creation of an Islamic state throughout the territory. The charter rejects peace negotiations and international initiatives that involve ceding any part of Palestine, considering them contrary to the movement's doctrine and religious faith. Jihad is seen as the only solution to the Palestinian problem. Despite its initial stance, later documents reveal an evolution in Hamas' thinking, with a greater emphasis on state-building and some nuance towards resistance and a two-state solution. Although theoretically separate from the Muslim Brotherhood, in practice, Hamas became

increasingly intertwined with the parent organisation. Hamas' initial leadership consisted of Shaykh Ahmad Yasin and six other founding members. Later, wings and committees were set up to deal with political issues, security, military operations, and the media. Overall leadership is vested in a *majlis shura* (advisory council), made up of members from both inside and outside the occupied territories. Hamas has built a vast institutional network that provides social services, including mosques (through al-Mujamma"), medical and educational institutions (such as the Islamic University of Gaza) and political institutions (such as university student parties) (Hroub 2006).

Hamas has gained credibility because of its active role in the Intifada and its relationship with the Muslim Brotherhood. Hamas' institutional network allows it to publicize its ideas, gather supporters, and provide social services. Sectoral elections in professional associations, trade unions, and student councils indicate the growing popularity of the movement. After the failure of the Oslo process and the start of the second Intifada in 2000, some polls suggested that support for Hamas had equaled that of Fatah (Robinson 2004).

On an international level, Hamas has historically been interlinked with the Muslim Brotherhood in Jordan, which has provided it with doctrinal, political, moral, and material support. The movement has also received support from Islamic movements in several Arab countries and in Islamic communities in Europe and the United States. Relations with Saudi Arabia and the Gulf states deteriorated after the Gulf War, while relations with Iran improved. Iran came to be singled out as a supplier of military training and financial support to Hamas. Hamas' sources of funding include local contributions, donations from individuals and Islamic movements abroad, as well as support from certain governments (Abu-Amr 1993).

After the Israeli withdrawal from Gaza in 2005, Hamas won the majority in the legislative elections in January 2006. In 2007, after clashes with Fatah, Hamas took control of the Gaza Strip. Since then, Hamas has ruled the region. This Hamas takeover in 2007 solidified the political and administrative division of Palestine (Atiya 2024).

With the handover of control of Gaza to Hamas in 2007, Israel imposed a tight and comprehensive blockade on the Gaza Strip, significantly limiting the movement of people and goods. The Gaza Strip, where Hamas exercises power, is a densely populated area with a large proportion of Palestinian refugees. Living conditions in the Gaza Strip under Hamas rule are difficult, with high unemployment rates and a shortage of resources, exacerbated by the blockade. Infrastructure, including wastewater treatment plants, has suffered damage due to the conflicts (Bjur 2014).

Hamas is considered by some to be an Islamic fundamentalist jihadist terrorist organisation whose main goal is the destruction of Israel. Hamas has been involved in repeated confrontations with Israel, including the launching of rockets into Israel

and military confrontations that have resulted in various Israeli operations against Gaza, such as the 2008-2009 war and other conflicts. Some authors suggest that the Israeli policy of containment may have inadvertently allowed Hamas to develop its military capacity (Finn Ostendorff 2016).

Despite the blockade and conflicts, Hamas also engages in political activities, such as sponsoring forums and events, and is seen by some Palestinians as a legitimate resistance force against the occupation. Hamas differentiates between the idea of the movement and its organisation. Hamas' goal is the liberation of Palestine and the foundation of an Islamic state. In 2005, Hamas accepted the terms of agreement based on the 1967 borders, the right of return for refugees, East Jerusalem as the capital of Palestine, and the release of prisoners, while also reaffirming the right to build military capacity (Rojas and Matta 2016).

The Hamas takeover of Gaza in 2007 followed a period of growing tension with Fatah, culminating in a confrontation that solidified the administrative and political division of the Palestinian territories. Hamas considers armed resistance to be a legitimate means of liberating Palestine. Hamas has managed to draw global attention to the Palestinian cause through its actions in Gaza. However, the elimination of Hamas as a goal for the future of Gaza is considered impractical by some, given that its ideology is deeply rooted in the Palestinian population. The future of the Gaza Strip, however, will have to be determined by the Palestinians themselves (Milton 2024).

## Conclusion

This study sought to understand how Egyptian rule, Palestinian control, and Hamas governance have shaped the socio-political landscape of the Gaza Strip and influenced the Palestinian struggle for self-determination. The analysis showed that each of these phases of governance had significant impacts, not only on administration and living conditions, but also on the consolidation of a national identity centered on resistance.

Egyptian rule (1948-1967) was a phase of indirect administration, during which Gaza remained on the margins of a real process of institutional development, but which laid the foundations for incipient forms of political organisation. With the subsequent Israeli occupation and the challenges posed by repression and the economic blockade, a collective feeling of resistance emerged. This culminated in the First Intifada, the founding moment of modern Palestinian national consciousness.

The establishment of the Palestinian Authority, resulting from the Oslo Accords, represented an attempt at self-government which, although symbolic, failed to guarantee effective sovereignty or institutional stability. Its limitations were exacerbated by factors such as corruption, political fragmentation, and the

continued Israeli occupation. In this context, the rise of Hamas from 2006 onwards represented not only a change of power but also a transformation of the very concept of governance in Gaza, merging civil administration with armed resistance. This duality had contradictory effects: it galvanized part of Palestinian society, while polarizing the territory and hampering efforts at internal reconciliation and international negotiations.

By revisiting the central question – how did these different phases of governance shape Gaza? – the results indicate that they all contributed, to varying degrees, to the construction of a collective identity centered on resistance and the quest for self-determination. The historical context provided by Egyptian rule, the expectations (and disappointments) of Palestinian governance, and the polarizing impact of Hamas reveal a trajectory where resistance is not only a reaction to external oppression but also a response to the crisis of internal legitimacy.

Furthermore, the effects of these phases on the socio-economic dimension have been profound. Poverty, unemployment, and dependence on international aid increased as a result of fragmented governance and the continuing Israeli blockade, particularly after 2007. These factors aggravated the vulnerability of the population and strengthened the link between material deprivation and political mobilization, especially among young people.

The applications of this research are diverse. By shedding light on how the different regimes have influenced the political structure and identity in Gaza, the study offers analytical tools for policymakers and international actors who want to intervene more effectively in the Israeli-Palestinian conflict. An informed understanding of the historical and social roots of the resistance can lead to more sensitive approaches, centered on the real aspirations of the Palestinian people.

However, the study has limitations. The emphasis on historical governance structures may have overlooked the current role of grassroots movements and civil society, which continue to shape the political space in Gaza. Furthermore, the analysis is predominantly based on secondary sources and the historic dimension, and does not fully reflect contemporary dynamics and the perceptions of the current population.

For future research, it is proposed to explore the role of community organisations and youth movements in building alternative forms of resistance and governance. Studies on the influence of international aid and external pressures, as well as comparative analyses with other regions under occupation or in a situation of prolonged blockade, could offer additional insights and generate innovative strategies for promoting peace.

In short, this study has revealed the intricate relationship between governance and resistance in the Gaza Strip, emphasizing how the legacies of different administrations

have shaped not only local institutions but also the collective identity of the Palestinian people. Understanding this trajectory is essential to addressing current challenges and charting paths towards a more just and peaceful future.

## References

**Abu-Amr, Ziasd.** 1993. "Hamas: A Historical and Political Background." *Journal of Palestine Studies* 22 (4): 5-19. https://doi.org/10.2307/2538077.

**Abu-Nimer, Mohammed.** 2002. "Dialogue in the Second Intifada: Between Despair and Hope." *The Alqsa Intifada*

**Asali, Muhammad, Aamer Abu-Qarn, and Michael Beenstock.** 2024. "Violence and cooperation in geopolitical conflicts: Evidence from the Second Intifada." *Journal of Economic Behavior & Organization* 217: 261-286. https://doi.org/10.1016/j.jebo.2023.11.012.

**Atiya, Nadiyah.** 2024. *The Origin of Hamas: An Israeli Creation*. https://www.researchgate.net/publication/385780041.

**Bjur, Becky.** 2014. "Gaza Strip History."

**Hancock, Landon E., and Joshua N. Weiss.** 2011. "Prospect Theory and the Failure to Sell the Oslo Accords."

**Farraj, Khalid.** 2019. "The First Intifada (Part II): The Road to Oslo." *Journal of Palestine Studies* 49 (1): 93-100. https://doi.org/10.1525/jps.2019.49.1.93.

**Farraj, Khalid.** 2017. "The First Intifada: Hope and the Loss of Hope." *Journal of Palestine Studies* 47 (1): 86-97. doi:10.1525/jps.2017.47.1.86.

**Feldman, Ilana.** 2008. *Governing Gaza: Bureaucracy, Authority, and the Work of Rule, 1917-1967*. Durham: Duke University Press.

**Finn Ostendorff, Tyler.** 2016. "Palestine, the Intifadas and Israel."

**Freas, Erik.** 2017. "The Six Day War and Its Aftermath." In *Nationalism and the Haram al-Sharif/Temple Mount*, by Erik Freas. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-319-49920-8_7.

**Goldstein, Yossi.** 2018. "The Six Day War: The War That No One Wanted." *Israel Affairs* 24 (5): 764-784. doi:10.1080/13537121.2018.1505475.

**Haun, Phill.** 2023. "Near-Catastrophic Victory: Disregarded Lessons from the." *Defence Studies* 215-237. https://doi.org/10.1080/14702436.2023.2199982.

**Hroub, Khaled.** 2006. "A 'New Hamas' through Its New Documents." *Journal of Palestine Studies* 35 (4): 6-27. https://doi.org/10.1525/jps.2006.35.4.6.

**Junka, Laura.** 2006. "The Politics of Gaza Beach: At the Edge of the Two Intifadas." *Third Text* 20 (3-4): 417-428. doi:10.1080/09528820600855428.

**Martinelli, Martín Alejandro.** 2022. *Palestine (and Israel), between intifadas, revolutions and resistance.* Luján: Editorial Universidad Nacional de Luján.

**Milton, Samson.** 2024. "Rethinking the "Day After" in the Gaza Strip: Learning from Previous Rounds of Reconstruction." In *Gaza's Cycle of Destruction and Rebuilding*, by Ghassan Elkahlout, 225-240. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-67198-2_12.

**Naser-Najjab, Nadia.** 2020. "Palestinian Leadership and the Contemporary Significance of the First Intifada." *Race and Class* 62 (2): 61-79. https://doi.org/10.1177/0306396820946294.

**Robinson, Glenn E.** 2004. "Hamas as a Social Movement."

**Rojas, René, and Nada Matta.** 2016. "The Second Intifada: A Dual Strategy Arena." *European Journal of Sociology* 57 (1): 65-113. https://doi.org/10.1017/S0003975616000035.

**Sabel, Robbie.** 2022. *International Law and the Arab-Israeli Conflict.* Cambridge: Cambridge University Press.

**Salihu, Jacob Tsunda.** 2024. ""Historical Foundation of the Israel-Palestine Conflict"." https://doi.org/10.13140/RG.2.2.17835.25122.

**Sotirović, Vladislav B.** 2024. "From the History of Israeli-Palestinian Conflict: The First Palestinian Intifada against the State of Israel (1987-1993) and Its Political Consequences."

**Sprague, Kalyn.** 2013. "Principled Pragmatism: Lessons Learned from the First Intifada."

**Yossef, Amr.** 2006. "The Six-Day War Revisited."

**ACKNOWLEDGEMENTS**

We would like to acknowledge the support of the Military Academy Research Centre (CINAMIL) and the Superior Institute of Social and Political Sciences (ISCSP) at the University of Lisbon, which has been instrumental in the completion of this research.

**FUNDING INFORMATION**

The authors declare that no funding or financial support was received from any organisation, institution, or individual for the research, design, execution, or writing of this work.

**CONFLICT OF INTEREST STATEMENT**

The authors declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

**DATA AVAILABILITY STATEMENT**

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analyzed specifically for this research.

**DECLARATION on AI use**

The author confirms that AI tools, including language models such as ChatGPT, Notebooklm and DeepL, were used solely to enhance the writing process, improve readability, and assist with grammar and formatting. All intellectual content, analysis, and critical arguments are the result of the author's original work. The AI tools were not used to generate research findings or substitute independent scholarly work.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Literature Survey on Meteor Burst Communication System

**Assist. Prof. Muhanned AL-RAWI, PhD***

*Bandung Institute of Technology, Department of Electrical Engineering and Informatics, Bandung City, Indonesia
e-mail: muhrawi@yahoo.com

## Abstract

A technology that has taken many years to develop is the foundation of Meteor-burst Communications (MBC). Many MBC systems have been installed and tested successfully. MBC systems comprise dynamic vehicular networks, fixed station networks, and point-to-point links. Currently available systems include medium data rate message handling, low data rate telemetry, and high-speed conversational voice advancements. In addition to describing the systems and technology currently being developed, this paper summarises earlier work in the field.

**Keywords:**
meteor burst communication; literature survey; applications.

**Article info**
Received: 12 May 2025; Revised: 4 June 2025; Accepted: 6 June 2025; Available online: 27 June 2025

Citation: Al-Rawi, M. 2025. "Literature Survey on Meteor Burst Communication System".
*Bulletin of "Carol I" National Defence University*, 14(2): 215-222. https://doi.org/10.53477/2284-9378-25-24

# 1. Introduction

The radio propagation mode known as meteor burst communications (MBC), or meteor scatter communications, uses the ionised trails left by meteors during atmospheric entry to establish short communication links between radio stations up to 2,250 kilometres (1,400 miles) apart. Radio waves can scatter either forward or backwards, as seen in Fig.1.

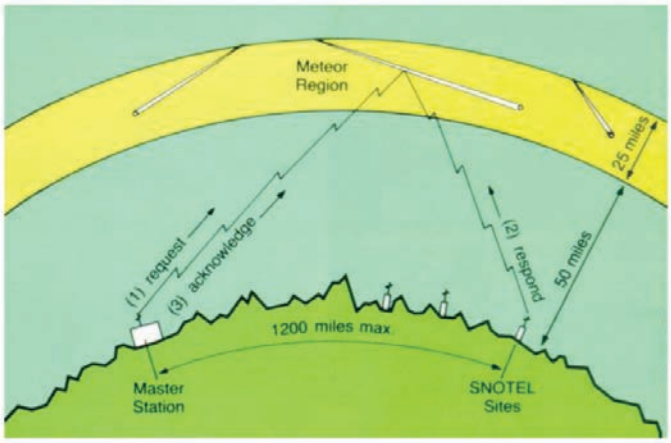



**Figure 1** Meteor scatter propagation

### *1.1. How Meteor Communication Works*

Millions of particles called meteoroids, that enter the Earth's atmosphere daily as it travels through space, have characteristics that make them suitable for point-to-point communication. In the E layer of the atmosphere, these meteoroids produce a luminous trail of ionised particles known as a meteor when they start to burn up. This trail may last for several seconds. Radio waves can be reflected by the ionisation trails because they can be extremely dense. The intensity of the ionisation produced by the meteor, which is frequently a function of the particle's initial size, determines the frequencies that can be reflected by any given ion trail. These frequencies are typically between 30 MHz and 50 MHz.

The altitude at which the ionisation occurs, the location of the meteoroid's descent over Earth's surface, the angle of entry into the atmosphere, and the relative positions of the stations trying to establish communications all affect the distance over which communications can be established. These ionisation trails provide only fleeting windows of communication opportunity because they only last anywhere from a few seconds to fractions of a second.

### *1.2. Military Use*

One of the first significant deployments was "COMET" (COmmunication by MEteor Trails), which was used to communicate over long distances with the headquarters of NATO's Supreme Headquarters Allied Powers Europe. With stations in the United Kingdom, France, Italy, West Germany, Norway, and the Netherlands, COMET

started operations in 1965. Depending on the season, COMET maintained an average throughput of 115–310 bits per second.

Beginning in the late 1960s, as satellite communications systems became more widely used, interest in meteor burst communications declined. It was discovered in the late 1970s that the satellites were not as widespread in their utility as first believed, particularly in areas with high latitudes or signal security considerations. Due to these factors, although its continued functionality is unknown, the U S. Air Force installed the Alaska Air Command MBC system in the 1970s.

More recently, Science Applications International Corporation (SAIC) established a testbed called the Advanced Meteor Burst Communications System (AMBCS) with Defence Advanced Research Projects Agency (DARPA) funding. AMBCS significantly increased the data rates, averaging 4 kbit/s, by using phase-steerable antennas pointed at the appropriate region of the sky for each time of day, in the direction that the Earth is moving "forward.". Satellites are significantly more expensive to operate, even though their nominal throughput may be roughly 14 times that of terrestrial networks.

The application of real-time steering could theoretically lead to further throughput gains. The fundamental idea is to aim the antenna at the precise location of the ion trail, or in certain situations, multiple trails at once using backscattered signals. Gain is increased as a result, enabling significantly higher data rates. According to what is currently known, this strategy has not yet been tested experimentally.

***1.3. Armature Radio Use***

The majority of meteor-scatter communication takes place between radio stations that follow a strict transmission and reception schedule. Stations attempting meteor-scatter communications must repeatedly transmit the same information until they receive an acknowledgement of reception from the other station because it is impossible to predict whether a meteor trail will be present at a suitable location between two stations. To control the flow of information between stations, established protocols are used. A complete information exchange frequently takes multiple meteors and a considerable amount of time to accomplish, even though a single meteor may produce an ion trail that supports multiple steps of the communication protocol.

Meteor-scatter communications can be conducted using any type of communications mode. In order to communicate with other stations during meteor showers without arranging a schedule beforehand, amateur radio operators in North America have been using single-sideband audio transmission. Morse code has been more widely used in Europe, where amateur radio operators have been sending messages at up to 800 words per minute using modified tape recorders and later computer programs. In order to replicate the transmission's content, stations that receive

these informational bursts record the signal and replay it more slowly. Voice and Morse code communications have been supplanted by a number of digital modes implemented by computer programs since 2000. The WSJT-X software implements MSK144, the most widely used mode for amateur radio operations.

## 2. Literature Survey

This section elaborates briefly on the previous works related to the meteor burst communication system in the current century.
The possibility of creating a communication channel through meteor bursts has been known for decades, according to research done by the authors in (Fabrés, et al. 2002). The idea of providing new wireless services at a low cost has sparked renewed interest in recent years. In order to meet the strict size requirements while maintaining good gain and polarisation purity, this paper suggests a novel mobile terminal antenna.

The article in (Antipov 2006) examines the ways to boost the throughput of meteor burst communication as well as the prospects for expanding its active radius. It is demonstrated how to reduce the error of time standard synchronisation by way of the meteor burst channel.

In (Yabin, et al. 2010), the geometry relationship between the heliocentric and geocentric space of sporadic meteors is constructed, and the development of modelling meteor radiant distributions is examined. Theoretical prediction models are developed for the channel parameters of Meteor Burst Communication (MBC). The MBC links use these models. These models predict outcomes that are in good agreement with observational data. The channel parameters' prediction models, which are provided here, can be useful in building a meteor communication system.

The variable rate data transmission should be used to increase the system average throughput in light of the meteor burst channel's characteristics (Cai, et al. 2010), which causes equalisation and channel tracing issues at the receiver. Though it is thought to be the best detection method, the joint data and channel estimation of maximum likelihood sequence detection using the per-survivor processing (PSP) principle has significant computational complexity, which makes it difficult to keep up with the meteor channel's decline. A few states in the trellis diagram are selected by the time-varying threshold based on the exponential decay of meteor channels, and the adaptive state reduction of the PSP (ASRP) algorithm is used based on the estimation of the system parameters. ASRP is demonstrated to be able to provide dependable data transmission for adaptive modulation and coding of the meteor burst communication system while also offering a good trade-off between computational complexity and performance.

In (Li and Zhu 2010), the authors employ high-speed wired links to connect the base stations in accordance with the ring topology structure in order to overcome the network reliability issues. They also construct a meteor burst communication network using the stop-wait protocol. Based on the Opnet platform, the authors examine and model the packet length and rate.

A novel automatic repeat request (ARQ) scheme, called the Go-Back-i-symbol (GBi) ARQ scheme, was proposed by the authors in (Mukumoto, et al. 2012) and is appropriate for Meteor Burst Communications (MBC). The scheme uses the Viterbi decoding algorithm for convolutional codes to achieve symbol-wise ARQ. For packet communications over time-varying short burst channels, like meteor burst channels, we also suggest a workable transmission protocol that applies the GBi-ARQ scheme. Computer simulations are utilised to assess the fundamental performance of the GBi-ARQ scheme in MBC. By contrasting the performance of the GBi-ARQ scheme with that of a traditional block-wise ARQ scheme, its effectiveness is demonstrated.

OPNET-based channel modelling and simulation for meteor burst communications are proposed in the paper (Yi, et al. 2015). In order to develop a realistic simulation scenario of meteor burst communications, multi-layer node models of the master station and slave station are presented after an analysis of the properties of the under-dense meteor burst channel. The simulation procedures for both full-duplex and half-duplex communication are used to carry out the simulation. The findings showed that full-duplex communication outperforms half-duplex communication in terms of effectiveness and that the OPNET-based channel model is very well-suited for meteor burst communication.

The authors in (Sulimov, et al. 2017) discuss the issue of nonreciprocity of propagation conditions in MBCSs, or meteor-burst communication systems. Previously, this issue had not received enough attention in publications. Advanced communication systems like meteor key distribution systems, which are designed to safely generate two identical copies of a shared secret key at both channel sides, and meteor synchronisation systems, which have nanosecond precision, may be significantly impacted by the channel nonreciprocity. The foundation of these systems is the processing of phase characteristics of meteor radio reflections, which require precise modelling. A rigorous solution to the issue of radio wave oblique diffraction on ionised meteor trails serves as the foundation for our new MBCS simulation model. A more thorough examination of the channel nonreciprocity effects is made possible by our diffraction approach, which enables more accurate simulation of the amplitude and phase characteristics of oppositely propagating signals. The authors demonstrate the adequate immunity of MBCS to ionospheric disturbances even when operating in harsh polar region conditions by presenting some initial simulation results on the channel nonreciprocity at meteor-burst propagation.

The purpose of the research in (Wada, et al. 2018) is to investigate whether Meteor Burst Communications (MBCs) could be used in equatorial areas. In Indonesia, researchers set up the remote and master stations in Jimbaran on Bali Island and Yogyakarta on Java Island, respectively. They verified, as a preliminary experimental result, that meteor burst channels were used to transmit some packets between the two stations.

The purpose of the article in (Voronin, Doroshenko and Ksenofontov 2019) is to support the value of using meteor communication networks as a basis for communication on the access connectivity network for vessel traffic management along the northern sea route's coastal zone on the route to the Arctic Russian infrastructure. From the perspective of system analysis, it gives us the generalised mathematical model of the network made up of the radiotransmitter and receiver, antenna systems, and structural-functional scheme, which are the main options that describe the telecommunication technologies of meteor connection. Using adaptive antenna grids as UHF antenna systems is such an example.

The technology for building a promising code division multiplexing meteor-burst communication system (MBCS) is presented in the paper (Holovan and Kharchenko 2020). In addition to improving the system's noise immunity and covert operation, it expands the bandwidth. Software-defined radio (SDR) is the foundation of the suggested technology, which uses software parameter control of the signals and their transfer protocols to enable MBCS adaptation to environmental conditions. It involves the best possible reception and matched digital filtering of large-base signals, and it includes a method for creating a large ensemble of signals with a direct sequence spread spectrum and enhanced auto- and cross-correlation properties. It is suggested to implement narrow-band interference rejection in the signal spectrum in conjunction with matched filtering software to increase noise immunity. The methods for synchronisation and detection that functioned well under non-Gaussian and non-stationary interference conditions were taken into account. A pseudorandom permutation of codeword elements of a maximum-length register code has been used in software to create a large ensemble of direct sequence spread spectrum signals with enhanced auto- and cross-correlation properties. Field-programmable gate arrays (FPGAs) have been used to implement algorithms for digital matched filtering and interference rejection as applied to large-base signals, which were designed using fast Fourier transforms. Software based on an FPGA has been developed for the detection and synchronisation of large-base signals.

The first attempt to investigate the potential existence of ionised meteor trails that offer combined forward and backwards scattering of radio waves at radio links larger than 300 km is made by the authors in (Lapshina, et al. 2021). The authors suggest a model for their computer simulation and refer to these meteor trails as "Forward-Backward Scattering," or simply FBS-trails. According to the authors, there are a number of real-world uses for the FBS-trails, such as accurate time synchronisation

of passive remote stations. According to simulation results, the nearly transverse orientation of the FBS-trails with respect to the axis of the meteor-scatter radio link is their most dependable distinguishing characteristic. FBS-trails are less likely to occur over longer radio links, and nearly all detections come from meteor trails that only provide forward scattering, which is the only direction of travel. Between one percent (at meteor-scatter links longer than 1500 km) and roughly ten percent (at meteor-scatter links shorter than 150 km), the proportion of FBS-trails in the total number of detected meteor events varies with link length.

Applying a multi-receiver system to the MBC is suggested in the paper (Takumi, Kaiji and Tadahiro 2023), which also examines three approaches for combining each receiver's reception: individual reception, soft value combining, and log-likelihood ratio combining. By considering the position distribution of meteor bursts and the direction of each receiving antenna, the paper illustrates the communication performance of the multi-receiver system using the three combining methods in MBC.

Through an analysis of the technology's principles, features, application scenarios, and emerging trends, the paper in (Gao 2024) came to the conclusion that meteor trail communication is a viable way to connect locations that are challenging to reach with other means. Additionally, this paper highlights certain shortcomings that could be improved in the future, allowing MBC to increase its effectiveness and adapt to more circumstances after resolving the current issues. This paper attempts to inspire experts who are willing to improve MBC by providing them with useful information by summarising all those aspects of this technology. This will enable them to create a better communication network using the modified MBC system.

## 3. Summary

This paper dealt with one of the most important technologies in the field of telecommunication systems, which is meteor bust communication system. The paper explained how this technology works and its applications in military use and amateur radio use. Also, the paper briefly described some of the previous works in the technology mentioned.

## References

**Antipov, I.E.** 2006. "Expansion of the Application Fields and Development Perspectives of Meteor Burst Radio Communication and Synchronization." *16th International Crimean Microwave and Telecommunication Technology.* Sevastopol, Ukraine. pp. 967-968. doi:10.1109/CRMICO.2006.256279.

**Cai, Jueping, Zan Li, Xiaojun Chen, and Benjian Hao.** 2010. "An adaptive receiver of joint data and channel estimation for meteor burst communications." *International Journal of Communication Systems* 24 (6): 745-760. http://dx.doi.org/10.1002/dac.1182.

**Fabrés, Marta Cabedo, Juan Escudero Vilar, Miguel Ferrando Bataller, and Alejandro Valero Nogueira.** 2002. "Novel mobile terminal antenna for meteor burst communication systems." *Microwave and Optical Technology Letters* 34 (2): 80–83. http://dx.doi.org/10.1002/mop.10378.

**Gao, S.** 2024. "Analysis and Application of Meteor Burst Communication." *2024 4th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS).* Shenyang, China. pp. 800-804. doi:10.1109/ACCTCS61748.2024.00147.

**Holovan, O.V., and V.M. Kharchenko.** 2020. "Constructing technology of a meteor-burst communication system with code division multiplexing." *RADIOFIZIKA I ELEKTRONIKA* 25 (2): 74-81. http://dx.doi.org/10.15407/rej2020.02.074.

**Lapshina, I., S. Kalabanov, A. Karpov, and A. Sulimov.** 2021. "Analysis of meteor trails providing combined forward and backward scattering of radio waves", ." *Planetary and Space Science* Vol. 195. https://doi.org/10.1016/j.pss.2020.105135.

**Li, Qing, and Lidong Zhu.** 2010. "Modeling and simulation of Meteor Burst Communication network." *2nd International Conference on Signal Processing Systems.* Dalian, China. pp. 332-335. doi:10.1109/ICSPS.2010.5555792.

**Mukumoto, Kaiji, Shinsuke Nagata, Tadahiro Wada, and Koji Ishibashi.** 2012. "Proposal of Go-Back-i-symbol ARQ Scheme and its Performance Evaluation in Meteor Burst Communications." *IEEE Transactions on Communications* 60 (8): 2336-2343. doi:10.1109/TCOMM.2012.071912.110330.

**Sulimov, Amir I., Arkadiy V. Karpov, Irina R. Lapshina, and Rustem G. Khuzyashev.** 2017. "Analysis and Simulation of Channel Nonreciprocity in Meteor-Burst Communications." *IEEE Transactions on Antennas and Propagation* 65 (4): 2009-2019. doi:10.1109/TAP.2017.2669730.

**Takumi, Kayama, Mukumoto Kaiji, and Wada Tadahiro.** 2023. "A Study on Application of Multi-Receiver System in Meteor Burst Communication." *IEICE Tech. Rep.* 122 (429): 7-12.

**Voronin, S., V. Doroshenko, and Y. Ksenofontov.** 2019. "Radiochannels of Meteor-Burst Communication Network of the Northern Sea Route." *Proceedings of Telecommunication Universities* 5 (3): 13-18. doi:10.31854/1813-324X-2019-5-3-13-18.

**Wada, Tadahiro, Kaiji Mukumoto, Hiroki Wadaguchi, I Wayan Mustika, and Linawati.** 2018. "Preliminary experiment of meteor burst communications in equatorial region."." *IEICE Communications Express* 7 (2): 43-47. http://dx.doi.org/10.1587/comex.2017xbl0136.

**Yabin, Zhang, Hu Dazhang, Lin Leke, and Guo Yuquan.** 2010. "Diurnal Variability Prediction Model of Meteor Burst Communication Channel." *Chinese Journal of Space Science* 30 (1): 60-65. http://dx.doi.org/10.11728/cjss2010.01.060.

**Yi, Zhao Xiang, Yong Xian, Xiong Mei Zhang, Hua Peng Zhang, and Xiao Dong Mu.** 2015. "Simulation and Analysis for Meteor Burst Communications Based on OPNET." *Applied Mechanics and Materials.* Vol. 738-739. pp.1205-1208. http://dx.doi.org/10.4028/www.scientific.net/amm.738-739.1205.

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

# The State of the Art in Sustainable Logistics: Economic and Military Perspectives

**LTC Daniela-Elena HRAB, PhD***
* "Carol I" National Defence University, Bucharest, Romania
e-mail: edaniela.hrab@gmail.com

## Abstract

The sustainable approach to logistics is emerging as a necessity in both the economic and military domains. This study aims to explore the current state of knowledge in the field of sustainable logistics within these spheres of activity, in order to identify gaps that should be addressed by future research. Based on a literature review methodology, the study brings to the forefront five thematic areas that have been addressed so far in the economic field, highlighting the need to extend them into the military domain as well. The analysis shows that the digitisation of logistics and the implementation of environmentally friendly technologies, which also reduce the negative impact on the health of end users, are two essential conditions for the transition toward sustainability. At the same time, the study emphasises the importance of an interdisciplinary approach and of researching the social impact of sustainable logistics, including the dimension related to humanitarian actions involving military forces. The main conclusion points to the need for clearly defining the concept of sustainable military logistics, taking into account developments in the economic environment and operational requirements.

**Keywords:**
logistics; defence; sustainability; sustainable development; alternative solutions; technologies.

**Article info**
Received: 12 April 2025; Revised: 5 May 2025; Accepted: 16 May 2025; Available online: 27 June 2025

Citation: Hrab, D.E. 2025. "The State of the Art in Sustainable Logistics: Economic and Military Perspectives". *Bulletin of "Carol I" National Defence University*, 14(2): 223-236. https://doi.org/10.53477/2284-9378-25-25

Sustainability is a concept common to both economic and military fields. From an economic perspective, it represents the ultimate goal of the sustainable development process (Blewitt 2018, 4-74), a higher form of economic development (Pezzey 1992, 10). This is characterised by a shift away from the sole objective of generating economic profit and by an increased concern for the environment and people, in order to ensure the long-term availability of natural resources (United Nations 1987, 16). In the military field, sustainability refers to the ability to support an operation with adequate combat power by providing the necessary human and material resources throughout its entire duration (NATO Standardization Office 2022, 399), with military logistics playing a key role.

Thus, in both fields, the concept of sustainability is related to the uninterrupted availability of necessary resources, the difference being that, in the military domain, sustainability focuses on the proper conduct of military operations, while the perspective of environmental protection and care for communities is less prominent. Nevertheless, considering that one of the 17 Sustainable Development Goals (SDGs) – specifically SDG no. 16 refers to ensuring peace, justice, and strong institutions (United Nations 2015, 25-26), it can be inferred that the military organization can contribute to creating the conditions for peace and, thereby, to those necessary for sustainable development. However, the potential for a broader contribution by the military organisation to the achievement of other SDGs should not be underestimated.

As for 2017, the issues related to logistics management and supply chain ranked among the top ten thematic areas of interest for researchers aiming to expand the knowledge in the field of sustainable development (Wichaisri and Sopadang 2017, 4). From the perspective of the integrated approach to the three pillars of sustainable development (economic, social, and environmental) (United Nations 2015, 1), economic entities have concluded that adopting a sustainable approach to logistics management can generate benefits both by increasing competitive advantage and by reducing environmental impact (Wichaisri and Sopadang 2017, 4-12), as well as by improving the efficiency of supply chains (Stroufe 2018, 326-329).

In the military domain, the way logistical support is provided can significantly contribute to the retention of human resources within the organisation (Vie, Trivette and Lathrop 2021, 28), thus offering benefits in terms of the sustainability of human resources. Moreover, the pursuit of sustainable logistical solutions is highlighted as a goal in strategic-level documents. For example, NATO envisions the development of environmentally friendly systems based on low-carbon technologies (NATO 2021), the use of alternative fuels (NATO 2020, 39-42), and contributions to enhancing the resilience of water and food sources (NATO 2016). The transatlantic vision is also shared at the EU level, where emphasis is placed on the procurement of environmentally friendly equipment, as well as on the requirement that the armed

forces of the member states develop strategies to combat climate change (European Union 2022, 5). Furthermore, the need for a sustainable approach at the EU level is explicitly stated in the recently issued White Paper. This document reflects ideals specific to sustainable development, such as improving the quality of life for European citizens and enhancing the security environment (European Commission 2025, 1).

Previous research also states that the need for sustainable military logistics is a real one. For instance, researchers point out that the successful completion of missions depends on the adoption of sustainable logistics practices, such as the use of technologies that reduce the need for petroleum-based supplies and the minimisation of material resource deployment (Mosher, et al. 2008, 51). In addition, sustainability is seen as a way to prevent illness among military personnel, caused by toxic spills, exposure to disease-carrying insects, poor sanitary conditions, and effects generated by improper hazardous waste management, which can also be exploited by the adversary (Mosher, et al. 2008, 5-6). As a result of the negative effects caused by extreme weather events, which sustainable development also aims to combat (United Nations 2015, 2-8), logistical processes such as resupply or maintenance can be disrupted due to breaks in the military supply chain (Best, et al. 2023, 22,73).

Based on the lessons identified by the U.S. military in Afghanistan and Iraq, shifting logistics toward sustainable solutions could help reduce equipment and personnel losses, as well as the massive consumption of fossil fuels (Harrington 2016). Consequently, there is a need to rethink the current methods of providing logistical support by adopting solutions that reduce the logistical footprint and carbon emissions, at the same time (Belcher, et al. 2019, 75-76). For example, the availability of alternative sources of water, electricity, and fuel could enhance the sustainability of logistical support (Cooper 2019, 4-7). As a result, the importance of this scientific endeavour lies in the need to establish a starting point for the implementation of the sustainable logistics objective, a goal that is increasingly evident both in civil society and in the military sphere.

In this context, the present study aims to explore the current state of knowledge in the field of sustainable logistics, in order to guide military logisticians' actions toward defining relevant and timely research problems (Kumar 2011, 17-27). To achieve this objective, the study employs the literature review method, following two main stages: 1) exploring the current state of knowledge and key scientific concerns in the civil domain of sustainable logistics; 2) analysing relevant studies in the field of sustainable military logistics.

Thus, using "sustainable logistics" as a search keyword in databases such as Google Scholar, ProQuest, Scopus, and Web of Science, several relevant studies were identified in the form of scientific articles or book chapters. The selection was based

on scientometric testing, taking into account aspects such as: the number of citations, the journal's impact factor relative to its field, the geographical distribution, and the preferences of researchers within the domain (Grigore 2021, 1-5). Studies with more than eight citations were considered. In the following sections, corresponding to the two stages previously mentioned, the content of these studies is analysed in order to identify the most significant findings and to establish the current state of knowledge in the field of sustainable logistics in the military area.

## State of research in the civilian field of sustainable logistics

Most studies on sustainable logistics were also conducted through the literature review method, and were focused on five main thematic lines. The first three addressed sustainable logistics in general, with particular emphasis on the environmental aspect (Ren, et al. 2019, 1-20), as well as alternative solutions for reducing the carbon footprint (Awwad, Shekhar and Iyer 2018, 584-591). The other two addressed the benefits of Industry 4.0 technologies in enhancing logistics sustainability (Sun, et al. 2022, 9560-91); (Grzybowska, Awasthi and Sawhney 2020, 1-18), and decision support systems in aid of sustainable logistics (Qaiser, et al. 2017, 1376-1388).

The first of the selected studies analysed articles in peer-reviewed journals published between 1999 and August 2019, identified in the Scopus and Web of Science databases. Using bibliometric analysis tools such as VOS (Visualization of Similarities), the study highlighted the growing interest in this field (Ren, et al. 2019, 2-4), as shown in Fig. 1.

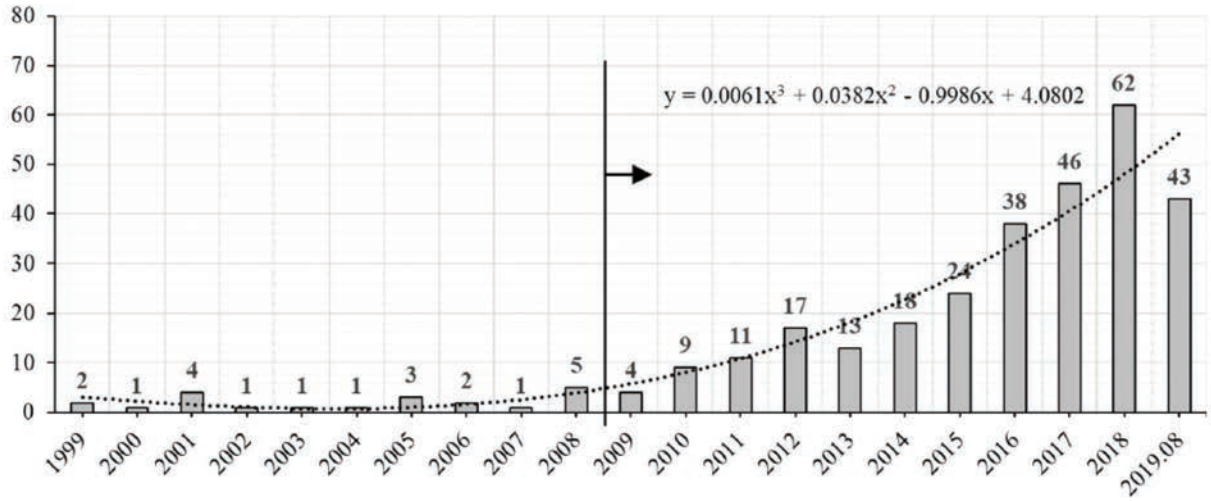



**Figure 1** The evolution of publications in the field of sustainable logistics, from 1999 to August 2019 (Ren, et al. 2019, 5)

By analysing a wide range of studies dedicated to sustainable logistics, it becomes evident that the aforementioned study is particularly relevant, serving as the foundation for subsequent research, as shown in Figure 2.

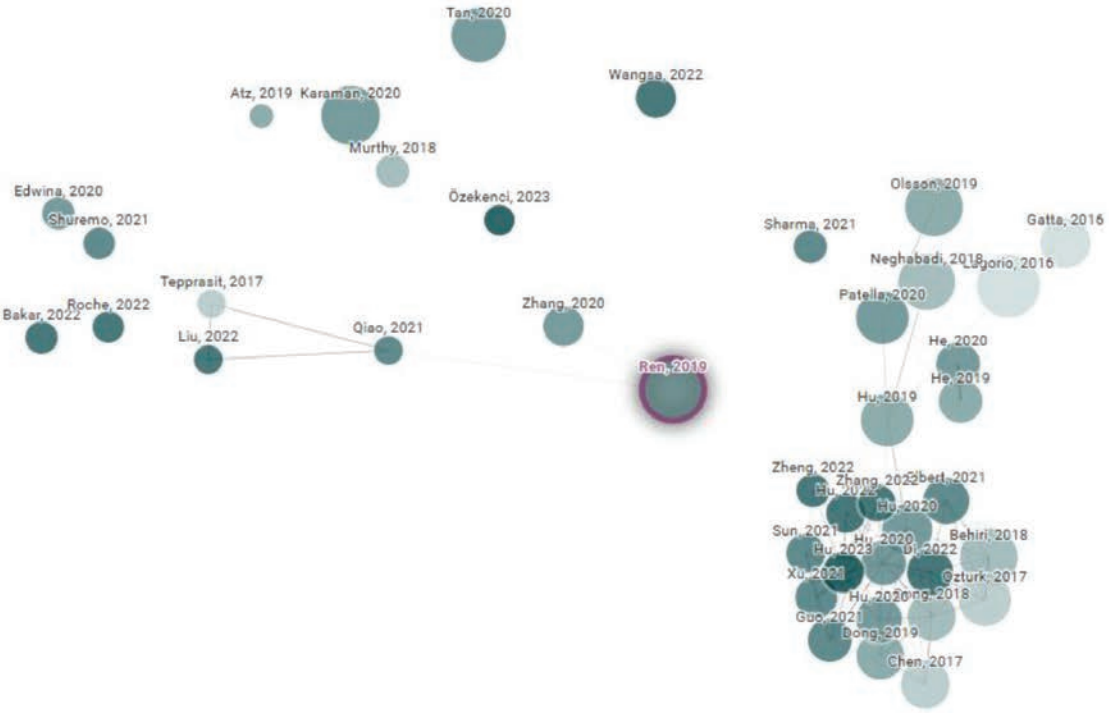



**Figure 2** Relevant publications on the topic of sustainable logistics (2016–2023).
Source: *Own analysis*, using https://www.connectedpapers.com/main/f90ddfa099de3c61a5ecb275d4a04e74323b2cd7/A-Systematic-Literature-Review-of-Green-and-Sustainable-Logistics%3A-Bibliometric-Analysis%2C-Research-Trend-and-Knowledge-Taxonomy/graph, accessed 10.03.2025

The study highlighted several subthemes within sustainable logistics research, corresponding to the environmental dimension of sustainability. The fifteen most relevant papers analysed by the authors, with citation counts ranging from 73 to 330, addressed topics such as green logistics, reverse logistics, and the environmental aspect of sustainable logistics. Most research efforts were concentrated in Europe, but those from China and America were also noteworthy (Ren, et al. 2019, 8-11). By thematically grouping the analysed studies, it becomes apparent not only that there is a strong focus on the environmental side of logistics sustainability, but also that there is a limited number of studies offering an integrative perspective on this field.

Within the thematic area focused on environmental protection, also, another study relevant to the issue of sustainable logistics suggests the use of green logistics mechanisms to reduce carbon emissions. The authors highlight the role of the "last-mile logistics" concept – which refers to the final segment in the supply chain specific to e-commerce (between the distributor and the end consumer) – in the generation of greenhouse gases, while also presenting solutions and strategies for reducing these emissions (Awwad, Shekhar and Iyer 2018, 586).

Regarding the negative environmental impact of this segment of the supply chain, the authors discuss solutions such as the use of alternative fuels, electric vehicles, urban distribution centres, and technology dedicated to optimising route selection (Awwad, Shekhar and Iyer 2018, 586). The focus is placed on analysing the characteristics of transport vehicles and delivery routes in order to choose the option that ensures the lowest fuel consumption, and, thus, the smallest carbon footprint (Awwad, Shekhar and Iyer 2018, 586). The proposed solutions are not universally applicable; the authors note that, under different circumstances, more efficient alternatives may exist (for example, hybrid vehicles may have a lower carbon footprint and do not require long battery charging times like the electric ones) (Awwad, Shekhar and Iyer 2018, 586). At the end of the study, authors highlight the need to identify barriers to implementing these solutions, as well as the importance of their comprehensive application in order to achieve conclusive results.

As time went by, beneficial changes have taken place, as evidenced by the existence of a study analysing the literature on the application of Industry 4.0 technologies for logistics sustainability, based on bibliometric and content analysis of publications. The issue of adopting technologies that facilitate the implementation of sustainability has thus emerged as a second main thematic area. According to the authors' analysis, 40% of researchers' concerns focused on the digitalization of logistics systems; 22.6% on interdisciplinary studies; 20.9% on sustainable transportation; 10.4% on sustainable production and procurement objectives; and the narrowest area of focus was sustainable warehousing, accounting for only 5.2% (Sun, Yu, et al. 2022, 9560-91).

Concerning the practical application of technologies for achieving logistics sustainability, the study highlights twelve innovative solutions explored by researchers between 2017 and 2020 (Sun, Yu, et al. 2022, 9560-91). This reflects a strong orientation of civil logistics toward harnessing the benefits of digitalisation and technological advancement to achieve sustainability. Despite the numerous concerns regarding the importance of implementing Industry 4.0 technologies for reaching sustainability goals, the study points out a lack of focus on identifying the challenges brought by this transformation (Sun, Yu, et al. 2022, 9560-91). In other words, while considerable scientific effort has been devoted to theorising and demonstrating the benefits of integrating these technologies, the measures that need to be taken and their consequences have not been identified, representing significant gaps in the body of knowledge on sustainable logistics.

As a result, the authors propose the following future research directions: complementing the technological vision of Industry 4.0 with the human-centred approach of Industry 5.0 to support the social dimension of sustainable logistics; implementing decision-support algorithms that take into account the three dimensions of sustainable development; the need for in-depth analysis of the environmental footprint generated by the energy used for the production and recycling of goods; developing analytical models to optimize the implementation of

Industry 4.0 technologies; using digitalization to increase the autonomy of logistic systems; leveraging the advantages of implementing semi-autonomous transport solutions; paying greater attention to how Augmented Reality (AR) and Additive Manufacturing (AM) technologies can enhance logistics sustainability; developing the sustainable dimension of reverse logistics; and using Industry 4.0 Technologies to increase resilience under special conditions, such as pandemics (Sun, Yu, et al. 2022, 9560-91). Analysing the findings of this study, one can observe the enormous potential of innovative technologies to enhance logistics sustainability — a goal that seems almost impossible to achieve without implementing measures for the digitalisation of logistics.

Closely related to the perspective offered by Industry 5.0, a concept aligned with sustainable logistics is Logistics 5.0, which is focused on identifying environmentally friendly packaging, transportation, and storage solutions, as well as increasing care for consumers (Trstenjak, et al. 2022, 2). However, the technology component remains important in Logistics 5.0 as well, with studies showing that both the COVID-19 pandemic and the Russia-Ukraine war have highlighted the urgency of adopting smart logistics solutions (Jafari, Azarian and Yu 2022, 1-27). Therefore, sustainable logistics must address actions across the three pillars of sustainable development, as well as those specific to smart logistics.

Another paper focused on literature analysis concerning sustainable production and logistics in the context of the Fourth Industrial Revolution reinforces the role of automated processes in the implementation of sustainable management (Grzybowska, Awasthi and Sawhney 2020, 1-18). The mathematical and statistical techniques used by the authors also led to the identification of the historical evolution of the two concepts: sustainable production has been studied since 1987, while sustainable logistics emerged as a concept in 2004, being associated with green industry and the circular economy (Grzybowska, Awasthi and Sawhney 2020, 5). The study was based on a sample of 892 scientific papers produced by researchers from 91 countries, most of which were published in scientific journals, with the Journal of Cleaner Production and Sustainability ranking first and second. The authors also identified several phases in the academic interest in sustainability: the activation period (1980-2006), the growth period (2007-2015), and the expansion period (2016-2018). Sustainable logistics belongs to the third period, during which a trend toward replacing the term with "sustainable supply chain" was observed (Grzybowska, Awasthi and Sawhney 2020, 15).

The third important theme in the field of logistics sustainability, addressed in studies based on the analysis of relevant literature, is represented by decision support systems. From this perspective, as of 2017, researchers concluded that the benefits of using these systems for the implementation of sustainable logistics are real, considering the complexity of the decision-making process at the strategic, operational, and tactical levels, in the context of sustainable development (Qaiser, Ahmed, et al. 2017, 1).

Furthermore, the necessity of using a sustainable model for choosing between local and external suppliers is brought into discussion – one that allows for the consideration of the three dimensions of sustainability when analysing criteria such as costs and carbon emissions generated from the perspective of various modes of transportation and other logistics operations (Katiraee, et al. 2024, 13).

The tendency to identify tools that assist decision-makers in the effort to optimise costs and reduce the environmental impact of logistics, as well as the insufficient attention paid to the social dimension of sustainability (Qaiser, Ahmed, et al. 2017, 6) has also been highlighted. Thus, there is a need for a holistic exploration of the feasibility of using decision-making tools to achieve sustainable logistics (Qaiser, Ahmed, et al. 2017, 7). It is, therefore, essential to preserve all guiding principles of sustainable development, as an approach focused solely on one of its dimensions is insufficient.

From the perspective of strengthening the social dimension of sustainable logistics, more recent studies address a fourth thematic area, showing that personnel working in this field must benefit from decent, properly regulated working conditions, as they are involved in a wide range of operations, such as: storage management, route planning, production planning and scheduling, workforce management, and lot sizing (Prunet, et al. 2024, 18-19).

In addition to the studies previously presented, there have also been other research concerns, like humanitarian logistics, which is closely linked to the social dimension of sustainable logistics, thus representing the fifth main theme in this domain. The author investigates the possibility of considering sustainable humanitarian logistics as a distinct research field, focusing on the principles that should be upheld and the concrete possibilities for implementation. In this context, a systemic approach is highlighted as a favourable factor for implementing sustainability in humanitarian logistics, allowing for the consideration of all pillars of sustainable development (Remida 2015, 11-29).

The author also highlights three levels of objectives that can be targeted: at the strategic level, the integrative approach to the pillars of sustainable development; at the tactical level, which is closest to humanitarian logistics and its beneficiaries, the humanitarian actions; and at the "operational" level, systemically approached logistics, including planning, procurement, and other activities related to logistics subsystems (Remida 2015, 21).

In addition, the study draws attention to several characteristics of sustainable humanitarian logistics, highlighting its potential to broaden the spatial and temporal horizons, as well as the requirement to consider all involved stakeholders. For the sustainability of humanitarian logistics, the author emphasises the importance of applying principles such as: an interdisciplinary approach, a dual vision (immediate response and long-term effect, private and public effort), and the use of analogies

with other logistics systems from different fields, such as the military system. Although the study highlights the need to achieve long-term effects through joint exercises with military forces and by utilizing existing military infrastructure, it does not explore the possibility of adopting sustainable logistics models from the military sector, nor does it detail the sustainability of military logistics as a potential example for humanitarian logistics (Remida 2015, 26-27).

Remaining within the sphere of humanitarian logistics, a more recent study, based on modelling and a sociological questionnaire, advocates for the inclusion of disaster-related logistics (applicable in cases of natural or human-made disasters) in university programs, as a means of achieving sustainability, given the shortage of trained logisticians and the widespread use of untrained volunteers. At one point, the author concludes that the use of professionally trained logisticians can bring sustainability to any organisation, an observation that highlights the significant role of logistics in sustainable development. One of the limitations of this study is that it was conducted with respondents from the academic environment, without considering other actors such as those from military organisations, who are often involved in disaster relief activities and support for the affected population (Khan, et al. 2020, 1-30). Therefore, it can be considered that humanitarian activities within military logistics could be classified under the social dimension of sustainable military logistics, helping to complete the framework of this emerging concept.

## State of the art in the field of sustainable military logistics

In the second stage, aimed at identifying the state of knowledge in the field of sustainable military logistics, searches in databases such as Google Scholar and ProQuest were conducted. The identified studies were also ranked according to their contribution to advancing the state of knowledge, taking into account criteria such as the number of citations, year of publication, and the impact of the journals in which they appeared. Since, from a military perspective, the results were not as numerous as those found in the field of economically sustainable logistics, no publications analysing the relevant literature in this domain could be identified. The following section presents the main findings from the analysis of relevant works that have addressed the issue of sustainability within military logistics.

A valuable study for military logisticians aiming to improve the efficiency and sustainability in this field highlights the importance of multicriteria analysis in decision-making regarding the selection of suppliers and supply routes for military forces in the Iraq theatre of operations. The authors provide a definition of the sustainability of supply routes, which involves the rational use of resources, based on technological development, institutional adaptation, and investments (Alazzawi and Żak 2020, 578). Although the definition is general, the reference to resources, technology, institutions, and investments partially situates it in the context of sustainable development.

This aspect also emerges from the analysis of the criteria considered in the decision-making process, which are explicitly formulated around the ideas of economic efficiency and environmental protection (Alazzawi and Żak 2020, 579) However, there is a lack of reference to the social dimension of sustainable development, as aspects related to the human resources involved in establishing logistic support corridors and selecting suppliers, as well as the impact of these choices on the beneficiaries, are not taken into account.

Another study provides a detailed analysis of one of the innovative technological solutions that contribute to sustainability in logistics, namely: the use of 3D printers for manufacturing spare parts needed during military missions and ensuring the sustainable supply of such goods. The study is significant because it offers a literature review dedicated to this topic, examines the specific case of the supply chain for spare parts within the Dutch military, and provides access to expert insights obtained through structured interviews. These interviews were conducted following the analysis of 40 articles and 12 scientific papers selected from a total of 78,439 publications identified on this topic (Den Boer, Lambrechts and Krikke 2020, 1-11).

Although the authors argue for the sustainable potential of this technology in preventing disruptions in the supply chain, challenges such as the high costs associated with acquiring and maintaining 3D printers, sourcing energy, and identifying local partners point to the need for further research. This is necessary to address issues such as: outsourcing the production service or providing it through military specialists, storing and transporting raw materials, information security, availability of data on product specifications, obtaining certifications for manufacturing spare parts, and respecting the intellectual property rights (Den Boer, Lambrechts and Krikke 2020, 5-10).

Since the analysed studies showed that the biggest challenges related to the implementation of AM technology are linked to the manufacturers' willingness to disclose product specifications, and considering that the authors do not advocate this solution for industrial-level production, but rather for small quantities and complex operational situations, it follows that a possible remedy could lie in how contractual clauses are formulated. This aspect could represent a possible direction for further research, as the study highlights the need for digitalisation in the field of military logistics and cooperation with manufacturers, paving the way toward the alternative of sustainable procurement in the military sector (Den Boer, Lambrechts and Krikke 2020, 7-10).

Aside from the mentioned studies, there are a few other papers within the military field which are focused on sub-elements of sustainable logistics; however, these cannot be considered relevant, as they have not been cited or used in the development of other works.

## Conclusions

Considering the analysis conducted on studies from the civil domain of sustainable logistics, it can be concluded that future research should have an interdisciplinary character and should aim to maximise the potential for an integrative approach to the five identified thematic areas. At this point, two elements emerge as essential for progress in this direction: the digitalisation of logistics processes and the implementation of technologies that facilitate the transition toward sustainability. From this perspective, future research should focus on identifying the barriers (challenges) that hinder this transition. While the benefits of a sustainable approach to logistics are often emphasised, the same cannot be said about the consequences of this transformation. Therefore, future studies should address each challenge in parallel with the effects generated by the integration of sustainability.

Moreover, the results of these studies could support the aforementioned transformations within the decision-making process, enabling decision-makers to adopt informed choices that take into account both the reflection of the three dimensions of sustainable development at the logistics level and the implications of adopting appropriate technologies and the expected outcomes.

Insufficiently explored by previous studies, the social dimension of sustainable logistics must benefit from research that targets both the advantages for logistics employees and communities. One underexplored area in this regard appears to be humanitarian logistics. This thematic line also serves as a bridge between civil and military logistics, with recommendations from previous research focusing on identifying sustainable modes of operation, similar to those adopted by military structures. However, the lack of studies confirming how this is approached at the military level only reinforces the need for dedicated research in this area. Specifically, future studies could focus on identifying lessons learned from humanitarian actions involving military structures, which may have the potential to facilitate the integration of sustainability in both civil and military contexts. Additionally, less-studied aspects such as sustainable transportation, production, procurement, and storage should receive greater attention from researchers.

From the perspective of the analysed military studies, it can be considered that publications in the field of sustainable military logistics are scarce, lacking interconnection, and focusing on isolated elements drawn from the sphere of economic sustainable logistics. Addressing only two of the five thematic areas identified in the case of civil logistics (the need for the digitalization of military logistics to facilitate the integration of advanced technologies, and the use of decision-making criteria based on the three dimensions of sustainable development), research in the field of sustainable military logistics is still in its early stages. It follows that each of the activities falling under the five thematic areas addressed in civil logistics could represent a potential future research direction within military

logistics. Furthermore, to facilitate the adoption of sustainable logistics solutions, future research could focus on identifying ways to operationalise the concept of sustainable procurement in the military.

Last but not least, another conclusion drawn from the analysis of military publications is the need to define the concept of sustainable military logistics. Although the present study highlights a series of dimensions and subdimensions of this concept, mainly from the perspective of studies in the field of civil logistics, the consideration of these components in the context of military logistics must be grounded in impact studies that do not jeopardise the success of military operations.

**Acknowledgements**
This study includes parts of the Research Report No. 2, related to the doctoral thesis titled *"Integrated Management of Defence Resources in the Context of Sustainable Development,"* publicly defended in September 2024.

## References

**Alazzawi, Ali, and Jacek Żak.** 2020. "MCDM/A Based Design of Sustainable Logistics Corridors Combined with Supplier Selection. The Case Study of Freight Movement to Iraq." *Transportation Research Procedia* (Elsevier) (47): 577-584. https://www.sciencedirect.com/science/article/pii/S2352146520303331.

**Awwad, Mohamed, Abhijeet Shekhar, and Abhishek Sundaranarayanan Iyer.** 2018. "Sustainable Last-Mile Logistics Operation in the Era of E-Commerce." *Proceedings of the International Conference on Industrial Engineering and Operations Management.* Washington DC, SUA. 584-591. http://ieomsociety.org/dc2018/papers/179.pdf.

**Belcher, Oliver, Patrick Bigger, Ben Neimark, and Cara Kennelly.** 2019. "Hidden Carbon Costs of the „everywhere war": Logistics, geopolitical ecology, and the carbon bootprint of the US military." *Transactions of the Institute of British Geographers* 45 (1): 65-80. https://rgs-ibg.onlinelibrary.wiley.com/doi/10.1111/tran.12319.

**Best, Katharina Ley, Scott R. Stephenson, Susan A. Resetar, Paul W. Mayberry, Emmi Yonekura, Rahim Ali, Joshua Klimas, et al.** 2023. *Research Report: Climate and Readiness. Understanding Climate Vulnerability of U.S. Joint Force Readiness.* RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1551-1.html.

**Blewitt, John.** 2018. *Understanding Sustainable Development.* Ediția a treia. Londra, New York: Routledge, Taylor & Francis Group.

**Cooper, Bradley.** 2019. *Precision Logistics: Sustainment for Multi-Domain Operations.* Institute of Land Warfare, The Association of United States Army, 1-8. https://www.ausa.org/sites/default/files/publications/SL-19-4-Precision-Logistics-Sustainment-for-Multi-Domain-Operations.pdf.

**Den Boer, Jelmar, Wim Lambrechts, and Harold Krikke.** 2020. "Additive manufacturing in military and humanitarian missions: Advantages and challenges in the spare parts supply chain." *Journal of Cleaner Production* (Elsevier). https://www.sciencedirect.com/science/article/abs/pii/S0959652620303486.

**European Commission.** 2025. "Joint White Paper for European Defence Readiness 2030." Bruxelles, 1-23. https://defence-industry-space.ec.europa.eu/document/download/30b50d2c-49aa-4250-9ca6-27a0347cf009_en?filename=White%20Paper.pdf.

**European Union.** 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/sites/default/files/documents/strategic_compass_en3_web.pdf.

**Grigore, Dan Radu.** 2021. „Evaluare și scientometrie." https://mepopa.com/Pdfs/dgrig21apr.pdf.

**Grzybowska, Katarzyna, Anjali Awasthi, and Rapinder Sawhney.** 2020. *Sustainable Logistics and Production in Industry 4.0. New Opportunities and Challenges.* Springer. https://link.springer.com/content/pdf/bfm:978-3-030-33369-0/1.

**Harrington, Kent.** 2016. "US Navy Green Fleet Makes Biofuels the New Normal." Accesat Martie 10, 2025. https://www.aiche.org/chenected/2016/01/us-navy-green-fleet-makes-biofuels-new-normal.

**Jafari, Niloofar, Mathew Azarian, and Hao Yu.** 2022. "Moving from Industry 4.0 to Industry 5.0: What Are the Implications for Smart Logistics?" *Logistics* (MDPI) 6 (26): 1-27. https://www.mdpi.com/2305-6290/6/2/26.

**Katiraee, Niloofar, Nicola Berti, Ilaria Isolan, Martina Calzavara, and Daria Battini.** 2024. "A sustainable joint economic lot size model for supplier selection under carbon emissions: A case study." *Cleaner Logistics and Supply Chain* (Elsevier) 13: 1-14. https://doi.org/10.1016/j.clscn.2024.100187.

**Khan, Muhammad, Muhammad Sarmad, Sami Ullah, and Junghan Bae.** 2020. "Education for sustainable development in humanitarian logistics." *Journal of Humanitarian Logistics and Supply Chain Management* (Emerald Publishing Limited) 1-30. https://www.emerald.com/insight/content/doi/10.1108/JHLSCM-03-2020-0022/full/html.

**Kumar, Ranjit.** 2011. *Research Methodology. A Step-by-step Guide for Beginners.* Ediția a treia. Sage Publications.

**Mosher, David E., Beth E. Lachman, Michael D. Greenberg, Tiffany Nichols, Brian Rosen, and Henry H. Willis.** 2008. *Green Warriors: Army Environmental Considerations for Contingency Operations from Planning Through Post-Conflict.* RAND Corporation. https://www.rand.org/pubs/monographs/MG632.html.

**NATO.** 2016. "Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council." Warsaw. https://www.nato.int/cps/en/natohq/official_texts_133169.htm.

**___.** 2020. "NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General." https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-reflection-group-final-report-uni.pdf.

**___.** 2021. *NATO Climate Change and Security Action Plan.* https://www.nato.int/cps/en/natohq/official_texts_185174.htm?selectedLocale=en.

**NATO Standardization Office.** 2022. „AAP-06, Glosar de termeni și definiții NATO." 1-440. https://www.unap.ro/ro/news/aap6.pdf.

**Pezzey, John.** 1992. "Sustainable Development Concepts: An Economic Analysis." *World Bank Environment Paper* (The World Bank) (2): 1-92. Accesat Martie 10, 2025. https://documents1.worldbank.org/curated/en/237241468766168949/pdf/multi-page.pdf.

**Prunet, Thibault, Nabil Absi, Valeria Borodin, and Diego Cattaruzza.** 2024. "Optimization of human-aware logistics and manufacturing systems: A comprehensive review of modeling approaches and applications." *EURO Journal of Transportation and Logistics* (Elsevier) 13: 1-25. https://www.sciencedirect.com/science/article/pii/S2192437624000116?via%3Dihub#sec9.

**Qaiser, Fahham Hasan, Karim Ahmed, Martin Sykora, Alok Choudhary, and Mike Simpson.** 2017. "Decision support systems for sustainable logistics: a review and bibliometric analysis." *Industrial Management & Data Systems* 117 (7): 1376-1388. https://eprints.whiterose.ac.uk/115817/1/05042017%20IMDS%20SI%20on%20KB-DSS%20-%20IMDS-09-2016-0410%20-%20Final%20draft.pdf.

**Remida, Aimen.** 2015. "A Systemic Approach to Sustainable Humanitarian Logistics." În *Humanitarian Logistics and Sustainability, Lecture notes in Logistics*, de Matthias Klumpp, Sander De Leeuw, Alberto Regattieri și Robert De Souza. Springer.

**Ren, Rui, Wanjie Hu, Jianjun Dong, Bo Sun, Yicun Chen, and Zhilong Chen.** 2019. "A Systematic Literature Review of Green and Sustainable Logistics: Bibliometric Analysis, Research Trend and Knowledge Taxonomy." *International Journal of Environmental Research and Public Health* 17 (261): 1-20. https://www.mdpi.com/1660-4601/17/1/261.

**Stroufe, Robert P.** 2018. *Integrated Management – How Sustainability Creates Value for Any Business.* Ediția întâi. Emerald Publishing Limited.

**Sun, Xu, Hao Yu, Wei Deng Solvang, Yi Wang, and Kesheng Wang.** 2022. "The application of Industry 4.0 technologies in sustainable logistics: a systematic literature review (2012–2020) to explore future research opportunities." *Environmental Science and Pollution Research* (29): 9560–9591. https://link.springer.com/article/10.1007/s11356-021-17693-y.

**Trstenjak, Maja, Tihomir Opetuk, Goran Đukić, and Hrvoje Cajner.** 2022. "Logistics 5.0 Implementation Model Based on Decision Support Systems." *Sustainability* (MDPI) 14 (11): 1-19. https://www.mdpi.com/2071-1050/14/11/6514.

**United Nations.** 1987. *Report of the World Commission on Environment and Development: Our Common Future.* Oslo: Oxford University Press, 1-300. https://sustainabledevelopment.un.org/content/documents/5987our-common-future.pdf.

**___.** 2015. "Transforming our world: the 2030 Agenda for Sustainable Development." New York, 1-35. https://www.unfpa.org/sites/default/files/resource-pdf/Resolution_A_RES_70_1_EN.pdf.

**Vie, Loryana L., MAJ Eric V. Trivette, and Adam D. Lathrop.** 2021. "Department of the Army Career Engagement Survey. First Annual Report." https://talent.army.mil/wp-content/uploads/2021/11/DACES-Annual-Report_JUNE2021.pdf.

**Wichaisri, Sooksiri, and Apichat Sopadang.** 2017. "Trends and Future Directions in Sustainable Development." *Sustainable Development* (Wiley) 26 (1): 1-17. https://onlinelibrary.wiley.com/doi/10.1002/sd.1687.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# USA Counterterrorism and the CIA Detention and Interrogation Program – between Legislative Constraint and Exceptional Permissiveness

**Lucian BUCIU, PhD***

*Ministry of Internal Affairs, Bucharest, Romania
e-mail: buciu.lucian@yahoo.com

## Abstract

In the war launched against terrorism of Islamic fundamentalist origin in the wake of the terrorist attacks of September 11, 2001 (9/11), the US was under pressure of time to implement a series of exceptional measures to combat terrorists and protect the security of the American state.

To that end, US counterterrorism, in a time race against terrorists, was coordinated by the CIA through the operationalization of a series of enhanced interrogation techniques, an integral part of the Detention and Interrogation Program developed by the Agency.

Through the qualitative method of document analysis, this research aims to assess the effectiveness of the enhanced interrogation techniques developed by the CIA, simultaneously relying on a dual content analysis: on the one hand, an analysis of the first 10 findings of the Report of the US Senate Select Committee on Intelligence on the CIA's Detention and Interrogation Program and, on the other hand, an analysis of the evidence provided by top policy makers and former US intelligence operatives.

The novelty of the subject of this scientific contribution for the Romanian literature on American counterterrorism resides in the fact that, in order to maximize the degree of objectivity in assessing the effectiveness of the Agency's enhanced interrogation techniques, it confronts the legislative dimension highlighted by the Commission Report and the information-operational dimension supported by factual elements selected from key actors within the American intelligence.

**Keywords:**

CIA; USA; counterterrorism; enhanced interrogation; intelligence; legislation; exceptionality.

**Article info**

Received: 13 May 2025; Revised: 2 June 2025; Accepted: 11 June 2025; Available online: 27 June 2025

Citation: Buciu, L. 2025. "USA Counterterrorism and the CIA Detention and Interrogation Program – between Legislative Constraint and Exceptional Permissiveness." *Bulletin of "Carol I" National Defence University*, 14(2): 237-246. https://doi.org/10.53477/2284-9378-25-26

## 1. Conceptual delimitations and methodological instruments

Considering the numerous existing definitions of the concept of terrorism in political science research, without "any of them being unanimously recognized" (Bourdillon 2007, 45), this paper will work with the signified of terrorism, in the Saussurean sense, by referring to four defining elements retained from Bourdillon – a highly elaborated technique that uses violence to generate fear among a significant number of people. Terrorism is thus equated with an atypical, asymmetrical war: "It is a war without war, that is, without an identified front, without rules, without prisoners, in which everyone takes part, whether they want to or not" (Bourdillon 2007, 50).
At the same time, it is noteworthy that the political-religious motivations underlying the action of the perpetrators of this atypical war rather place terrorism under the sign of a "political-religious utopia" (Cusson 2018, 21). Hence, the success of a terrorist attack depends on the linguistic mastery with which the terrorist manages to verbalize the claim of political-religious victory, which means that we are dealing with terrorism that is "secretive in deeds and abundant in words" (Pascallon 2018, 46).

As regards the complexity of the terrorism typology, this research focuses on terrorism of Islamic fundamentalist origin in line with research in the field of security studies, which emphasizes a terminological mismatch between Islamic religion and terrorism: "It should be noted that, essentially, Islamic religion and terrorism are two conflicting terms. Islam condemns and rejects all forms of terror. Thus, it is not feasible to use certain expressions such as Islamic terrorism. Attempts to equate Islamic religion with terrorism are not only groundless and flawed, but also purely propagandistic and malicious" (Barna and Popa 2021, 32).

Counterterrorism, or what could be the antidote against terrorism of Islamic fundamentalist origin, will be understood throughout the entire scientific approach in the meaning proposed by *Law no. 535 of 25 November 2004 on preventing and combating terrorism, as subsequently amended and supplemented*, according to Article 4, as "all offensive measures carried out in the event of a terrorist act, aimed at releasing hostages, capturing or annihilating terrorists, neutralizing the devices used by them, freeing attacked or occupied targets and restoring law and order."

In terms of the methodological instruments used, this article is the result of a predominantly qualitative research, which chose to use the document analysis method. The research used the technique of both qualitative and quantitative content analysis, applied to the first 10 conclusions of the Commission Report, in order to make an inventory of the main arguments based on which the Commission measured mostly the ineffectiveness of the enhanced interrogation techniques developed by the CIA.
A qualitative content analysis will be devoted to the pleadings of former top decision-makers and US intelligence operatives directly or indirectly involved in the Agency's counterterrorist actions in order to identify the main elements that led them to support the effectiveness of the Agency's enhanced interrogation techniques.

The overarching aim of the research will thus be to determine the degree of effectiveness of US counterterrorism operationalized by the CIA under exceptional circumstances immediately after 9/11.
To this end, the analysis proposed by this paper will materialize against the background of the tension between two dimensions – on the one hand, the legislative dimension to which the Commission Report belongs, and on the other hand, the information-operational dimension to which the selection of relevant elements provided by former top decision-makers and operatives in the American intelligence is circumscribed.
Thus, the effectiveness of the Agency's enhanced interrogation techniques will be assessed by the extent to which their application produced or failed to produce intelligence, and whether or not they ultimately yielded counterterrorist successes.

## 2. Background of the preparation of the US Senate Select Committee on Intelligence Report on the CIA Detention and Interrogation Program

The 9/11 terrorist attacks in the US represented a zero time in resetting American counterterrorism in that the CIA, under exceptional circumstances and time pressure, operationalized a series of so-called enhanced interrogation techniques in the war on terrorism against the backdrop of strong social emotion: "This despicable attack killed nearly 3,000 people and shocked the American public, which was consumed with a burning desire for revenge" (Petraeus and Roberts 2025, 227).
The reset of American counterterrorism also entailed a fundamental reform of the American intelligence community with the *Intelligence Reform and Terrorism Prevention Act of 2004* when "Congress had mandated domestic intelligence collection" (Hayden 2018, 190) and the position of *Director of National Intelligence (DNI)* was established to replace the *Director of Central Intelligence (DCI).*

After Washington Post journalist Dana Priest began a so-called "Pulitzer parade with an expose of the CIA's detention and interrogation program in 2005" (Hayden 2018, 195), two years later, in 2007, former CIA Director Michael Hayden decided to release to members of the US Senate Select Committee on Intelligence the videotapes of detainees Abu Zubaydah and Abd al-Rahim al Nahiri at CIA headquarters (MacArthur and Horton 2015, 77). In 2009, the Commission launched an investigation into how enhanced interrogation techniques had been used by the CIA in the US-led war on terrorism: "on March 5, 2009, by a vote of 14 to 1, the Commission approved the task order of an inquiry into the CIA's Detention and Interrogation Program" (MacArthur and Horton 2015, 77).

In December 2012, 3 years after the start of the investigation and following intense analytical work on the CIA-operated detention and interrogation program, the report, including 20 findings and conclusions, was approved by a majority vote

of the Commission, chaired by Dianne Feinstein. In 2014, by a majority vote, the Commission submitted to the President "the revised version of the findings and conclusions and the executive summary of the report for declassification and public release" (MacArthur and Horton 2015, 80).
Thus, the "exceptional powers in combating the terrorist threat" (Rodriguez JR 2014, 164) that the CIA made use of will be specifically analyzed in this paper.
Furthermore, the analysis of the first 10 findings and conclusions of the Report of the US Senate Select Committee on Intelligence on the CIA Detention and Interrogation Program appears to be relevant also from the perspective of addressing the tension between legislative constraint/ethics versus exceptional permissiveness in the name of the US fight against terrorism.

## 3. Conclusions of the Report of the US Senate Select Committee on Intelligence regarding the CIA Detention and Interrogation Program

***3.1. "The CIA's use of its enhanced interrogation techniques was not an effective means of acquiring intelligence or gaining cooperation from detainees"*** (United States Senate 2014, 12).
By using the word "intelligence" seven times in the first conclusion of the Report, the Commission gradually tries to tip the balance towards the ineffectiveness of the Agency's enhanced interrogation techniques.
The key element on which the Commission reinforces its argument is the fact that the Agency applied said techniques on seven of the 39 detainees, and failed to obtain relevant intelligence.
The generalization of the ineffectiveness of enhanced interrogation techniques to an insignificant sample of seven out of a total of 39 Agency detainees is more indicative of a manifestly political intention of the Commission to dictate, from the very first conclusion, an approach that seems to tend towards rejecting the effectiveness of the CIA Program.

The Commission considers that the ineffectiveness of the CIA's enhanced interrogation techniques is psychologically justified by the fact that detainees, when regularly subjected to brutal, coercive treatment, often choose to communicate false or partially truthful information meant to confuse the interviewer and persuade him of the authenticity of what they are relating.
The review of the content of the paragraphs of this first conclusion did not reveal any concrete elements supporting the ineffectiveness of the Agency's techniques from the psychological point of view and in terms of false or partially truthful information.

In contrast, from the argument of former CIA Director Michael Hayden, which abounds in factual data, one will note that, based on the counterterrorist instrumentation operationalized by the CIA, almost 8,000 reports were produced,

with direct relevance to strengthening US security and deciphering the complex terrorist network (Hayden 2018, 427). A review of the very accurate, even mathematical argument of the former CIA director reveals an obvious refutation of the ineffectiveness of the Agency's enhanced interrogation techniques.

The exceptional quality of the intelligence obtained from the Agency's enhanced interrogations is additionally supported with field data by Jose A. Rodriguez Jr, former CIA counterterrorism chief: "The intelligence obtained from KSM, like that previously obtained from AZ, proved to be invaluable. 441 of the 1,700 footnotes in the 9/11 Commission Report came from interrogations of Al-Qaeda leaders" (Rodriguez JR 2014, 134).
But the pinnacle of the inestimable value of the intelligence obtained through the Agency's enhanced interrogation techniques led to the killing of Osama bin Laden on May 2, 2011, which de facto represented "the culmination of over a decade of intelligence work that had finally located him" (Petraeus and Roberts 2025, 255).

***3.2. "The CIA's justification for the use of its enhanced interrogation techniques rested on inaccurate claims of their effectiveness"*** (United States Senate 2014, 12-13).
The reference to five of the most important institutions of the American state – the White House, the National Security Council, the Department of Justice, the Office of the Inspector General of the CIA and Congress – in the second conclusion reinforces the Commission's plea regarding the ineffectiveness of the Agency's enhanced interrogation techniques and, at the same time, textually takes the form of a direct accusation made by the Commission against the CIA regarding the questionable legality of the counter-terrorist instruments operationalized under exceptional circumstances.
The textual tension gradually builds, with the Commission going so far as to assert that "the CIA's solution was simple – lie" (MacArthur and Horton 2015, 20) so as not to be legally prevented from implementing its arsenal of enhanced interrogation techniques.

Nevertheless, the factual arguments put forward by Jose A. Rodriguez Jr, head of the CIA's post-9/11 Counterterrorism Center, translate the indisputable effectiveness of the Agency's enhanced interrogation techniques: "Once he began to cooperate, the information willingly provided by AZ was some of the most important intelligence collected after 9/11" (Rodriguez JR 2014, 109).

***3.3. "The interrogations of CIA detainees were brutal and far worse than the CIA represented to policymakers and others"*** (United States Senate 2014, 13-14).
The Commission's predilection for the use of terms from the semantic field of brutality in the wording of its conclusion (such as "coercive", "physically harmful", "physical injury", "sleep deprivation", "waterboarding technique") can be interpreted as the Commission's intention to emphasize the inefficiency of the Agency's enhanced interrogation techniques.

In contrast to the above, when examining the arguments put forward by Jose A. Rodriguez Jr, former head of counterterrorism at the CIA, we will note the concrete example of the walling technique, which translates a categorical rejection of the so-called brutality of interrogations, as he proves with field data that "many of the techniques are essentially bluffing." (Rodriguez JR 2014, 103).

***3.4. "The conditions of confinement for CIA detainees were harsher than the CIA had represented to policymakers and others"*** (United States Senate 2014, 14).
The examination of the content of this conclusion reveals the Commission's predilection for the use of terms that fall within the semantic field of detention (such as "poor", "complete darkness", "isolated cells", "dungeon", "lack of human contact"), which could be interpreted as a direct accusation against the Agency by the Commission, which criticizes the CIA for having concealed the truth about the actual conditions of detention and the questionable psychological training of the interviewers who posed an extreme threat to the detainees' lives.

On the other side of the barricade, when analyzing the pleadings of Jose A. Rodriguez, Jr., the fallacy of the Commission's conclusion gradually becomes apparent, being strengthened by the former operative through the concrete example of the medical check-up: "[...] they were subjected to a thorough medical check-up to see if they had any medical condition that would have prevented, in their case, the safe application of the techniques" (Rodriguez JR 2014, 104).

***3.5. "The CIA repeatedly provided inaccurate information to the Department of Justice, impeding a proper legal analysis of the CIA's Detention and Interrogation Program"*** (United States Senate 2014, 14-15).
The Commission's predilection for using terms from the semantic field of legality (such as "justice", "incorrect", "verification", "torture", "prohibition", "memorandum") in the substantiated text of this conclusion once again highlights the Commission's accusation towards the CIA Program's questionable legality.

Based on the evidence emerging from the review of the official documents made available to them, the members of the US Senate Select Committee on Intelligence on the CIA's Detention and Interrogation Program raise a series of incriminating arguments against the Agency, claiming that "CIA legal experts lied in every instance to deceive the Office of Legal Counsel within the Justice Department, ostensibly to get the approval they needed" (MacArthur and Horton 2015, 17).

In return, the defense of the former operative Jose A. Rodriguez Jr. based on concrete legislative elements tips the scales in favor of the legality of the Agency's Program, revealing that "the approval of the interrogation techniques came to us in the form of a memo from the Office of Legal Counsel within the Department of Justice" (Rodriguez JR 2014, 104).

***3.6. "The CIA has actively avoided or impeded congressional oversight of the program"*** (United States Senate 2014, 15-16).
The insistent use of the word "inaccurate", four times in the last but one paragraph of this conclusion, simply translates the Commission's accusations about the questionable legality of the instruments used by the CIA under the Detainee Detention and Interrogation Program approved by former US President George W. Bush.
By using negative verb forms (such as – "the CIA did not brief", "the CIA did not respond") as well as terms that can be categorized as belonging to the semantic field of rejection ("resisted", "refusing", "declined to answer"), in the content of this conclusion, the Commission manages to even more obviously reinforce its accusations against the Agency on the unclear legal framework surrounding enhanced interrogation techniques.

In opposition to the Commission, in analyzing Jose A. Rodriguez Jr.'s argument, one will note the reference to Presidential Executive Order MON, by which former President Bush granted exceptional powers to the CIA after 9/11 to wage the war on terrorism (Rodriguez JR 2014, 164). At the same time, former CIA Director Hayden, by textually employing a presentative construction, merely highlights the importance of the exceptionality of the instrumentalization of enhanced interrogation techniques that is above and beyond any accusation regarding the questionable quality of the legislative framework, in light of what happened on 9/11: "This is not the President's program. This is America's program."

***3.7. "The CIA impeded effective White House oversight and decision-making"*** (United States Senate 2014, 16-17).
The symmetrical use of the terms "inaccurate" and "incomplete" in the first and last paragraphs of this conclusion indicates a gradual textual tension which effectively translates a kind of indictment of the Commission against the Agency for incomplete and inaccurate information to the White House on the effectiveness of enhanced interrogation techniques.

This conclusion of the Commission could also be contradicted by reference to Jose A. Rodriguez Jr' defense, of which the example of the presidential authorization coming from the White House will be noted, which reflects a reinforcement of the legality of the counterterrorist instruments operated by the CIA in exceptional circumstances after 9/11: "Less than a week after the September 11 attacks, the President formally authorized us to capture, extradite, and interrogate terrorists" (Rodriguez JR 2014, 71).

***3.8. "The CIA's operation and management of the program complicated, and in some cases impeded, the national security missions of other Executive Branch agencies"*** (United States Senate 2014, 17-18).
From the review of the content of this conclusion, it gradually emerges that a semantic field of constraint ("complicated", "impeded", "restricted", "denied", "blocked") is taking shape, which translates the Commission's strong criticism

of the exceptional powers bestowed on the CIA by former President Bush to fight terrorism, by putting into practice the tools of enhanced interrogation techniques. The Commission is opposed to the exceptionality of action granted to the Agency, pointing out that the FBI is also part of the US intelligence community and therefore can successfully execute counterterrorism missions on behalf of the US.

From the review of the factual arguments put forward by former CIA counterterrorism chief Jose A. Rodriguez Jr., it is obvious that he is firmly opposed to the Commission's above argument, and is clearly in favor of the exceptional powers granted to the Agency in the war on terrorism: "The FBI's mindset is to gather information that can be used to prove a crime in court. CIA officers focus on gathering intelligence to prevent new acts of terrorism" (Rodriguez JR 2014, 93).

***3.9. "The CIA impeded oversight by the CIA's Office of Inspector General"*** (United States Senate 2014, 18).
The progressive build-up of a semantic field of reticence ("avoided", "resisted", "impeded") as well as the repeated use of the term "inaccurate" in the second paragraph, textually captures the accusatory position of the Commission chaired by Dianne Feinstein on the legality of the CIA's enhanced interrogation techniques, alleging the inexistence of oversight of the Agency's Program by the CIA's Office of Inspector General.

From the analysis of Jose A. Rodriguez Jr's pleading, it becomes apparent that he is in antithesis to what the Commission claims, as the former CIA operative delivers specific arguments in favor of the legality of the CIA's enhanced interrogation techniques: "Less than a week after the September 11 attacks, the president formally authorized us to capture, extradite, and interrogate terrorists" (Rodriguez JR 2014, 71).

***3.10. "The CIA coordinated the release of classified information to the media, including inaccurate information concerning the effectiveness of the CIA's enhanced interrogation techniques***" (United States Senate 2014, 18-19).
The repetitive use of the word "inaccurate" in the last paragraph of the conclusion highlights the Commission's strongly incriminating position towards the Agency, which is being harshly accused of leaking false classified information to the media, obviously intended to strengthen the notable successes in US counterterrorism achieved by the operationalization of the CIA's enhanced interrogation techniques approved under exceptional circumstances at presidential level.

The analysis of Jose A. Rodriguez Jr.'s argumentation reveals the very direct and tough manner in which he firmly rejects the fact that the Agency is responsible for a possible leak of classified information to the media and admits that such speculation seriously damages the CIA's image (Rodriguez JR 2014, 227), a position that former CIA Director Hayden seems to visibly adhere to, as it emerges from the examination of the specific arguments he delivers: "I have told journalists that a recent avalanche

of articles has cost us five promising counterterrorism and counterproliferation sources who feared we could not guarantee their security. [...] When a covert CIA presence in a no-go zone was revealed in the media, two local sources were arrested and executed" (Hayden 2018, 137).

## Conclusions

In order to maximize objectivity in assessing the degree of effectiveness of the enhanced interrogation techniques operationalized by the CIA after 9/11, this research concurrently focused on a double analysis: on the one hand, the analysis of the first 10 conclusions of the Report of the Commission chaired by Diane Feinstein and, on the other hand, the analysis of the arguments of former key players at the top of the CIA leadership.

Against the backdrop of the textual-discursive tension between the political-legislative dimension in which the conclusions of the Senate Committee Report fall and the informative-operational dimension that includes the arguments of important former CIA actors, the evaluation of the degree of efficiency of the CIA's enhanced interrogation techniques led to the highlighting of two polarized camps: on one side are those on the Senate Committee chaired by Feinstein, who argue for the ineffectiveness of the CIA's enhanced interrogation techniques; they are opposed by former key players and operatives who argue for the effectiveness of the counterterrorism operationalized by the CIA after 9/11.

Without in any way discounting the procedural shortcomings from a legislative point of view in the operationalization of the CIA's enhanced interrogation techniques under exceptional conditions, against the clock, and considering that the Agency's interrogations produced extremely useful intelligence that was subsequently used and led to the killing of Osama bin Laden on May 2, 2011, it can be concluded that the CIA's enhanced interrogation techniques produced intelligence and ultimately proved to be effective in achieving their ultimate goal.

## References

**Barna, C., and A. Popa.** 2021. *Forme de manifestare a terorismului în societatea contemporană.* București: Editura Top Form.

**Bourdillon, Y.** 2007. *Terrorisme de l'Apocalypse. Enquête sur les idéologies de destruction massive.* Paris: Ellipses.

**Congress.gov.** 2004. *Legea privind reforma serviciilor secrete și prevenirea terorismului din 2004.* Retrieved from https://www.congress.gov/bill/108th-congress/senate-bill/2845

**Cusson, M.** 2018. *L'antiterrorisme à l'âge du djihadisme.* Paris: L'Harmattan.

**Hayden, M. V.** 2018. *Pe muchie de cuțit. Serviciile secrete americane în epoca terorii.* București: Editura Meteor Press.

**MacArthur, J. R., and S. Horton.** 2015. *La CIA et la torture.* Paris: Les Arènes.

**Parlamentul României.** 2004. *Legea nr. 535 din 25 noiembrie 2004 privind prevenirea și combaterea terorismului, cu modificările și completările ulterioare.* Publicat în Monitorul Oficial nr. 1.161 din 8 decembrie 2004. Retrieved from https://legislatie.just.ro/Public/DetaliiDocumentAfis/57494

**Pascallon, P.** 2018. *Rendre le renseignement plus efficace dans la lutte contre le terrorisme.* Paris: L'Harmattan.

**Petraeus, G. D., and A. Roberts.** 2025. *Conflict. Evoluția războiului din 1945 până la luptele din Gaza.* București: Litera.

**Rodriguez JR, J. A.** 2014. *Măsuri extreme. Cum au salvat măsurile dure adoptate de CIA după 11 septembrie viețile cetățenilor americani.* București: Editura RAO.

**Șandor, S. D.** 2013. *Metode și tehnici de cercetare în științele sociale.* București: Editura Tritonic.

**United States Senate.** 2014. *Report of the Senate Select Committee on Intelligence. Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, together with Foreword by Chairman Feinstein and Additional and Minority Views.* Unclassified. Retrieved from https://www.intelligence.senate.gov/sites/default/files/publications/CRPT-113srpt288.pdf

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

# On Cyber Vulnerabilities Management in Critical Sectors: the Health Sector

**Irina-Delia NEMOIANU, PhD***
*Romanian National Cyber Security Directorate
e-mail: irina.nemoianu@dnsc.ro

## Abstract

The digitalisation of the Romanian health sector has accelerated significantly, especially in the aftermath of the COVID-19 pandemic, but this transition has amplified cybersecurity risks, exposing critical infrastructures and patient data to persistent threats. This study analyses the technical and non-technical vulnerabilities of the medical sector, based on both documentary research and a survey conducted among representatives of health institutions. The results highlight important challenges, ranging from the use of outdated software, shortages of specialised cybersecurity staff and significant variations in the level of maturity of cyber protection between public and private organisations. Given the diversity of challenges identified, the resilience of the health sector requires an integrated cybersecurity strategy, underpinned by technological investments, continuous training and coherent risk management policies.

**Keywords:**
cybersecurity; cyber-attacks; vulnerabilities; the health sector; resilience; the human factor.

**Article info**
Received: 31 March 2025; Revised: 29 April 2025; Accepted: 6 May 2025; Available online: 27 June 2025

Citation: Nemoianu, I.D. 2025. "On Cyber Vulnerabilities Management in Critical Sectors: the Health Sector". *Bulletin of "Carol I" National Defence University*, 14(2): 247-256. https://doi.org/10.53477/2284-9378-25-27

In a global context marked by technological advances, the digitalisation of the healthcare system has become a strategic priority for Romania, aiming to improve the quality and efficiency of healthcare services. This has been accelerated by the COVID-19 pandemic, which highlighted the need for the medical sector to adapt quickly to the new realities. However, the sector faces significant challenges in terms of cybersecurity, both in terms of infrastructure and human resources expertise.

Increased digitisation has led to the expansion of the attack surface for cyber threats, evidenced by the increasing number of cyberattacks on the Romanian healthcare system. The RO-CCH project (RO-CCH 2025a), funded by the European Union and implemented by the Romanian National Cyber Security Directorate (DNSC), addresses cybersecurity challenges in the health sector, with the aim of reducing cybersecurity risks and raising awareness in health institutions in Romania.

Based on the work carried out within the project, this article presents an analysis of cybersecurity vulnerabilities that can affect the health sector in Romania, highlighting the socio-technical dimensions. These dimensions reflect the interactions between technical components - hardware, software and network infrastructure - and social factors - such as human behaviour, organisational culture and the regulatory framework, and the need for an integrated approach to achieving the resilience of the sector. The study also integrates the results of a survey conducted with hospital representatives, highlighting their perception of cyber threats and the current capacity of organisations to manage vulnerabilities.

## Cyberattacks on the health system

The Romanian healthcare system is facing a significant increase in cyber threats, especially ransomware attacks, targeting both hospital IT infrastructures and IT service providers in the field. These trends are in line with European or global trends (ENISA 2023), where 8% of ransomware attacks in 2023-2024 targeted the health sector, the third most affected sector (ENISA 2024, 15). In Romania, the attacks demonstrated vulnerabilities in both data protection and continuity of regular operations, underlining the need for robust cybersecurity measures and recovery plans in case of an incident.

In July 2021, Witting Clinical Hospital No. 1 in Bucharest was the victim of a ransomware attack with the Phobos malware, which encrypted data on the institution's servers, with attackers demanding a ransom for decryption (SRI 2021). This ransomware, usually distributed by exploiting Remote Desktop Protocol (RDP), remote access vulnerabilities in Windows operating systems, functions as a Ransomware-as-a-Service (RaaS) platform (Cisco Systems Inc. 2023). Such platforms allow collaboration between developers and affiliates to extend attacks. The decentralised nature of the model makes it difficult to identify attackers and apply

countermeasures, and although the Romanian Intelligence Service (SRI) has provided recommendations for securing the IT infrastructure, the extent of the damage has not been made public. A similar incident occurred in 2023 at the 'Saint George' Recovery Hospital in Botosani, where the attackers encrypted the institution's database, seriously disrupting the activity and demanding a ransom of three bitcoins (approximately EUR 50,000) (ProTV 2023). This intensely publicised attack highlighted the severe impact of cyber threats on the Romanian healthcare system.

The latest large-scale ransomware attack took place between 11 and 12 February 2024, affecting Romanian Soft Company, the provider of the Hippocrates IT platform used by many public hospitals in Romania (DNSC 2024). The incident severely disrupted the work of 26 hospitals that depended on this platform for data management and coordination of medical services. The malware used was Backmydata, a variant of Phobos ransomware, similar to the one used in the 2021 attack on Clinical Hospital No. 1 Witting. At the time of writing, the exact cause of the incident was not publicly disclosed, but the DNSC noted that no evidence of data exfiltration had been identified. Thus, it remains uncertain whether the attack exploited a vulnerability of the platform, an erroneous configuration of the RDP or other human errors.

The increase in the frequency and complexity of ransomware attacks on the IT infrastructure in the Romanian medical sector highlights the risks associated with deficiencies in cybersecurity and supply chain vulnerabilities. Recent attacks highlight the need to implement strategies to protect hospital networks, including implementing strict data backup and recovery policies to prevent losses from ransomware attacks, protecting computer services exposed to the internet, or connecting to internal networks through secure Virtual Private Network (VPN) connections. Other measures that ensure resilience in case of materialised attacks can be increased investments in advanced cybersecurity solutions and rapid incident response plans, as well as training IT and medical personnel to detect and prevent common cyber threats, starting with phishing.

## Cyber vulnerabilities

In cybersecurity, vulnerabilities are structural weaknesses or errors in computational logic identified in software or hardware components that, when exploited, may compromise the confidentiality, integrity and availability of data and information systems. These weaknesses can result from design, implementation or configuration deficiencies and are access points for attackers.
Mitigating these vulnerabilities usually involves one or more of the following measures:

- Applying patches to fix errors in the code
- Modification of the technical specifications so as to reduce exposure to potential operations

- Impairment or complete removal of functionalities or protocols that present vulnerabilities

According to the Common Vulnerabilities and Exposures (CVE) programme (The MITRE Corporation n.d.; SecurityScorecard n.d.), managed by MITRE Corporation, each vulnerability is recorded under a unique CVE ID, which allows it to be associated with specific versions of the software or shared libraries, thus providing a reference system to assist in the vulnerability management process.

The Common Vulnerability Scoring System (CVSS) (NIST n.d.) provides a metric for assessing the severity of cybersecurity vulnerabilities based on several criteria such as their impact and exploitability. It can be translated into a qualitative representation (low, medium, high and critical) to help organisations assess and prioritise vulnerabilities in management processes. CVSS is a public standard developed by the Special Interest Group (SIG) and widely used by organisations around the world, the latest version being CVSS 4.0. Hospital IT systems can face numerous cyber vulnerabilities, many of which affect various hardware, software and network products widely used in other sectors, which can compromise patient data security and the functioning of critical healthcare infrastructure.

Following documentary research and discussions with cybersecurity experts working with health entities, the most common problems identified include the use of outdated software and hardware, exposed to risks due to a lack of updates and adequate technical support. Poor network security protocols, poor configurations and inadequate access control measures can also facilitate unauthorised access to computer systems. In addition, insufficient training of medical and administrative staff increases the vulnerability of health institutions to phishing attacks, which remain one of the main methods of compromising IT infrastructure. These shortcomings expose hospitals to significant threats such as data breaches, ransomware attacks and unauthorised access to sensitive information, underlining the need to implement effective and proactive cybersecurity measures.

The report (RO-CCH 2025b) outlines a number of cyber vulnerabilities related to hardware, software, network equipment or cybersecurity equipment that healthcare organisations can consider in their security strategies. In this context, certain vulnerabilities identified by the corresponding CVEs, whether historical or newly discovered, present a high (High) or critical (Critical) CVSS score that requires an urgent approach and effective mitigation measures, given the potential impact on the continuity of health services and the protection of critical infrastructure in the health sector. At the same time, new vulnerabilities are frequently made public, requiring an appropriate cybersecurity strategy, including tracking the alerts of various manufacturers or suppliers, informing various national security agencies, or acquiring/collaborating with organisations to obtain CERT-like services on vulnerabilities actively exploited by attackers.

An increasingly relevant approach in vulnerability management is the integration of artificial intelligence (AI) solutions into existing solutions (AI-driven vulnerability management) by using machine learning algorithms to improve vulnerability detection, prioritisation and remediation processes (Wan, et al. 2024). Thus, AI solutions can analyse in real time large amounts of data, from system and network logs to threat intelligence feeds, to identify patterns that suggest possible security weaknesses in the infrastructure. Commercial vulnerability management platforms such as Qualys VMDR, Tenable.io, Rapid7 InsightVM, or Darktrace have integrated machine learning algorithms to correlate known vulnerabilities with their level of active exploitation in the real environment (Tod-Răileanu, et al. 2024). Artificial intelligence can also be used in vulnerability prediction, which predicts the likelihood of a newly discovered vulnerability being exploited, based on the historical behaviour of attackers and associated attack vectors.

The digitalisation of the health sector also requires the integration of specific technologies, systems and protocols, such as pharmacy management systems, ambulance and emergency services, and laboratory information systems. Among the most important are Electronic Health Records, which integrate patient histories using standards such as HL7 (Health Level 7) for the exchange of information between systems such as Radiology Information Systems and Laboratory Information Systems. Systems such as Picture Archiving and Communication Systems (PACS) are used to store and manage medical imaging, while the Digital Imaging and Communications in Medicine (DICOM) standard enables interoperability between imaging devices and storage systems. These technologies represent an additional attack surface to be considered by organisations in the medical sector, both for hospitals, clinics and for medical imaging centres, medical analysis laboratories, dental practices.

## Vulnerabilities in medical devices

Modern medical devices such as heart monitors, ventilators and insulin pumps are increasingly integrated into the digital infrastructure of hospitals through the Internet of Medical Things (IoMT). This connectivity allows real-time monitoring of patients and automatic transmission of data to clinical information management systems, thereby improving the efficiency of healthcare. The devices communicate using standard protocols such as Wi-Fi and Bluetooth, as well as proprietary protocols developed by medical equipment manufacturers. This connectivity, while operationally beneficial, poses challenges in terms of cybersecurity, in particular in protecting the confidentiality, integrity and availability of patients' data.

To ensure secure transmissions, additional protection technologies such as VPNs and TLS/SSL encryption are also used over traditional network protocols such as TCP/IP, which allow communication between devices. These mechanisms reduce the risk of interception of sensitive information and protect against cyberattacks

targeting medical infrastructure. However, many IoMT devices remain vulnerable due to unsafe configurations, lack of software updates, or security standards that vary between different manufacturers.

A study of medical devices (Cynerio 2023) looked at the safety of medical devices in 14 NHS trusts, representing 6.4% of all NHS trusts, entities of the British health sector. These institutions were selected to reflect the diversity of hospitals in terms of size, number of beds and level of funding. The study used an anonymised analysis tool to identify the main risks, vulnerabilities and active threats associated with IoMT devices. The findings highlighted critical issues, including the possibility of exploiting unpatched vulnerabilities in more than 40 percent of devices, unsafe network configurations or the risk of unauthorised access. At the same time, more than 36.7% of devices would face reduced risks by implementing appropriate micro-segmentation at the network level.

## The Human Factor in Cybersecurity

Information systems in healthcare facilities are susceptible to a number of vulnerabilities originating from the human factor. These weaknesses, while not correlated with common vulnerabilities and exposures or specific CVEs, are a critical vector in cyber risk assessment. The analysis of these vulnerabilities requires a contextual approach, given the workflows and human interactions in the medical field.

Attack vectors and human errors in the hospital context: One of the predominant attack vectors is phishing campaigns, where staff are misled by means of e-mails imitating legitimate sources. This manipulation results in compromising authentication data or installing malicious software. In parallel, poor credential management practices, such as using poorly configured passwords or reusing them across multiple platforms, facilitate unauthorised access.

Internal threats and social engineering: Internal threats from employees with malign intentions or grievances pose a significant risk, as they may abuse access privileges to exfiltrate sensitive data or disrupt operations. In addition, social engineering techniques, which manipulate staff to divulge confidential information or perform actions that compromise security, underline the importance of awareness and continuous training.

Inadequate data management and shortcomings in staff training: Improper handling of sensitive data, by accidentally transmitting patient information through unsecured channels or unintentionally exposing it, is another category of risk. Shortcomings in cybersecurity training programmes contribute to this vulnerability, with staff often not familiar with the latest security threats and practices.

Weaknesses in access control and non-compliance with security protocols: Poor user access management, manifested by failure to update access rights following changes in roles or leaving the organisation, creates entry points for attackers. Failure to comply with security protocols, such as ignoring software updates or bypassing virtual private networks (VPNs), additionally exposes systems to known vulnerabilities.
Risks associated with mobile devices and unintended disclosure: The loss or theft of mobile devices containing sensitive data poses a considerable risk of information exfiltration. Also, unintentional disclosure of data through mis transmission or leaving screens unattended are additional risks that can be mitigated by implementing a security-oriented organisational culture.

## Perception of sector representatives on the level of cybersecurity

In recent years, in addition to the ransomware attacks that affected the activity of hospital units in Romania, organisations have been exposed to a variety of cyberattacks, highlighting an increasingly sophisticated threat landscape. One of the surveys conducted within the project with IT representatives and the management of 30 medical organizations in Romania generated data that provide clues on the level of preparedness of these organizations in the face of cyber threats, as well as on the perception of the subjects on the current state of cyber security in the sector.

According to responses collected from industry representatives, phishing and spear-phishing accounted for the largest share of reported incidents over the past three years, followed by Distributed Denial of Service (DDoS) attacks aimed at freezing IT infrastructures and brute force attacks used to compromise access credentials. Also, a significant category of threats was the distribution of malware and spyware, indicating a diversification of methods used by attackers. This hierarchy of incidents underlines the dynamic and adaptable nature of cyber threats as well as the need to implement multilateral security measures. In particular, the prevalence of phishing attacks justifies the need to consider human vulnerabilities as a vector of exploitation within cybersecurity systems.

Regarding the assessment and prioritisation of cyber vulnerabilities within organisations, participants provided varied answers on the existence of specific frameworks or methodologies used to determine the level of risk associated with each vulnerability. Of the 30 respondents, 12 said they did not have such a structured programme for managing vulnerabilities. However, around half of the participants use vulnerability scanning tools, intrusion detection systems (IDS) or other automated tools to identify risks and threats. These results point to a heterogeneous approach to cybersecurity in the sector, where, despite efforts to monitor threats,

a significant proportion of organisations are still not implementing a formalised vulnerability assessment and management process.

The low level of cybersecurity and the low capacity to manage incidents within organisations are attributed to a combination of technical, organisational and human factors. According to the data obtained, 28 out of 30 respondents indicated as main causes the use of obsolete or unsafe IT systems, the implementation of inadequate security controls and the limited resources allocated to the protection of the IT infrastructure. These factors not only increase the risk of compromising critical data and infrastructure but also make it difficult to implement proactive security measures.

A secondary but significant aspect identified in the analysis is the lack of cybersecurity awareness among employees, which contributes to additional vulnerabilities in the face of social engineering-based attacks such as phishing. These shortcomings reflect deeper systemic problems, in particular underfunding and underinvestment in cybersecurity infrastructure. In addition, they are amplified by human factors, including shortages of specialised staff, which limit the ability of organisations to effectively detect, prevent and respond to cyber incidents. The lack of a strategic commitment to developing a security-oriented organisational culture further aggravates risks, underlining the need for urgent measures to strengthen cyber resilience at institutional level.

## Conclusions

Romania has made significant progress in digitalising the health sector, accelerated by the COVID-19 pandemic; the transformation has, however, increased cyber risks, exposing networks and patient data to threats. In this article, we highlighted the technical and non-technical vulnerabilities of the sector, obtained both from documentary research and questionnaires with representatives from the sector. The highlighted problems of the sector, from the use of obsolete software to the lack of cybersecurity-trained staff in both the public and private sectors, underline the need for stricter measures to protect health IT infrastructure against growing threats.

To protect critical health infrastructure and patient data, effective vulnerability management, software upgrades and IT infrastructure upgrades are needed. Given the different levels of cybersecurity maturity of the organisations in the system, the resilience of the health system requires a coherent national strategy based on investment in technology, cybersecurity training and effective risk management policies.

As technology advances, the integration of artificial intelligence could play a decisive role in proactively addressing cyber risks, both in the health sector and in other critical sectors. By automating processes to identify risks and threats and prioritise

vulnerabilities, AI-enabled solutions can greatly improve responsiveness and operational efficiency. Adopting a national strategy that includes such technologies could be an asset for Romania in protecting critical infrastructures and increasing cyber resilience at the national level.

## References

**Cisco Systems Inc.** 2023. *Understanding the Phobos affiliate structure and activity.* https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/.

**Cynerio.** 2023. "The State of NHS Trust IoT Device Security 2023." https://www.cynerio.com/nhs-trusts-iot-security-report-cynerio-only.

**DNSC.** 2024. "Backmydata Ransomware (Alert)." https://www.dnsc.ro/vezi/document/alert-backmydata-ransomware-eng-pdf.

**ENISA.** 2023. "Enisa Threat Landscape: Health Sector." https://www.enisa.europa.eu/publications/health-threat-landscape.

**___.** 2024. "ENISA Threat Landscape 2024." doi:10.2824/0710888.

**NIST.** n.d. *CVSS – Vulnerability Metrics.* Accessed December 2024. https://nvd.nist.gov/vuln-metrics/cvss.

**ProTV.** 2023. *Spital din Botoșani, atacat de hackeri. Le-au criptat baza de date și cer 50.000 de dolari răscumpărare.* https://stirileprotv.ro/stiri/ilikeit/spital-din-botosani-atacat-de-hackeri-le-au-criptat-baza-de-date-si-cer-50-000-de-dolari-rascumparare.html.

**RO-CCH.** 2025a. *About RO=CCH.* https://rocch.ro/en/about-ro-cch.

**___.** 2025b. *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1).* RO-CCH - DIGITAL-2022-CYBER-02. https://rocch.ro/en/dissemination/deliverables/d2-1/download.

**SecurityScorecard.** n.d. *CVE Details.* Accessed December 2024. https://www.cvedetails.com/.

**SRI.** 2021. *Atac ransomware asupra Spitalului Clinic Witting din București.* https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html.

**The MITRE Corporation.** n.d. *CVE® Program Mission.* Accessed December 2024. https://www.cve.org/.

**Tod-Răileanu, Gabriela, Ana-Maria Dincă, Sabina-Daniela Axinte, and Ioan C. Bacivarov.** 2024. "Enhancing Vulnerability Management with Artificial Intelligence Algorithms." *International Conference on Cybersecurity and Cybercrime.* 96–101. doi:10.19107/CYBERCON.2024.13.

**Wan, Shengye, Joshua Saxe, Craig Gomes, Sahana Chennabasappa, Avilash Rath, Kun Sun, and Xinda Wang**. 2024. "Bridging the Gap: A Study of AI-based Vulnerability Management between Industry and Academia." *2024 54th Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S).* IEEE Computer Society. 80-87.

**FINANCING INFORMATION**

This research was partly made possible by the support of the RO-CCH project, which provided direct data on the management of cyber vulnerabilities in medical institutions in Romania through the *Cyber security Vulnerabilities Report for healthcare and health institutions (D2.1)*. The authors express their gratitude to health organisations and experts who contributed by participating in surveys and providing valuable insights.

The Romanian National Cyber Security Directorate (DNSC) is the beneficiary of a grant for the implementation of the project 'Romanian Cyber Care Health - RO-CCH' under Grant Agreement No 101101522. The project is financed by the Funding Authority: CNECT.H – Digital Society, Trust, and Cybersecurity, under call DIGITAL-2022-CYBER-02-SUPPORTHEALTH.

**DECLARATION ON CONFLICT OF INTERESTS**

The authors declare that there are no potential conflicts of interest regarding the research, paternity and/or publication of this article.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Countering the Glide Bombs Threat in the Ukrainian Conflict

**LTC Adrian MIREA, PhD***

*"Carol I" National Defence University, Bucharest
e-mail: mirea.adrian@yahoo.com

## Abstract

The integration of emerging technologies in the Ukrainian conflict plays an important role in the conduct of military actions and generally manages to capture the attention of military analysts in terms of characteristics, potential effects, or potential impact. Of similar importance in the conduct of the conflict is the revision or adaptation of old technologies to the current operational needs of force structures. The conflict in Ukraine provides the context for the revival and innovative use of classic weapon systems and munitions to meet the needs of combat forces. This paper deals with such an adapted use of classic aviation bombs in a gliding kit version, which has practically enabled the Russian Air Force to perform its basic missions in a new way. In the first phase, the focus of the paper is on describing the threat posed by glide bombs and their potential impact on the conduct of military actions, and in the second phase, I have presented possible ways of countering glide bombs, emphasizing the efforts of the Ukrainian forces and its allies to limit the number of glide bomb attacks. In carrying out the paper, I explored open sources of information through the method of documentary analysis in order to synthesize the most relevant aspects of the use and counteraction of glide bombs in the Ukrainian conflict. The results of the investigations emphasize the interest of the Ukrainian forces and their allies in identifying the most effective methods of adapting military actions to the new reality of the operational environment while also countering the threat posed by the mass use of glide bomb attacks.

**Keywords:**
glide bombs; aviation bombs; gliding kit; air defense; Ukrainian conflict.

**Article info**
Received: 15 May 2025; Revised: 30 May 2025; Accepted: 4 June 2025; Available online: 27 June 2025

Citation: Mirea, A. 2025. "Countering the Glide Bombs Threat in the Ukrainian Conflict"
*Bulletin of "Carol I" National Defence University*, 14(2): 257-266. https://doi.org/10.53477/2284-9378-25-28

In 2023, the Russian Army was reported to be using the UPAB-1500 aviation bombs (weighing 1500 kg) in a variant equipped with a gliding kit and with the possibility of GPS target guidance. These bombs were presented by the Russian military for the first time in 2019 at the MAKS exhibition (Gheja 2023), and currently their technical characteristics open new possibilities for attacking ground reinforced targets in the Ukrainian conflict, in particular due to their 1,010 kg explosive charge and the ability to launch accurately from a distance of 40 km. Despite the advantages provided by these characteristics, the Russian military underestimated the need for such glide bombs and other types of precision-guided munitions before the invasion of Ukraine in February 2022, as it was admitted by the commander of the Russian Air Forces (Hardie 2024).

In order to write this article, I explored open sources of information, generally publications, various websites, and authored works, sources detailing relevant aspects regarding the use of glide bombs in the Ukrainian conflict, as well as ways to counter such attacks. Based on the method of documentary analysis (Okoko, Tunison and Walker 2023, 140), I aimed to systematically collect, analyze, and interpret the data obtained from the mentioned sources, with the purpose of understanding and synthesizing the main elements of interest for the present paper.

The concept of using glide bombs is not new, the first successful attacks with such munitions being attributed to the Nazi armed forces (Fritz-X) in World War II. The design of the bomb began in 1939 (Australian War Memorial 2025) under the direction of Dr. Max Kramer, and final acceptance tests were carried out near Foggia in Italy, in early 1942. Operational use began in mid-1943, and the most successful glide bomb attack was recorded in September 1943, when three Fritz-X bombs struck and sank the Italian battleship, Roma.

Currently, glide bombs are launched from fixed-wing aerial platforms, usually jets. It is the speed and altitude at which aircraft launch these bombs that provide the gliding kit mounted on them with the energy needed to engage targets at considerable distances. At the same time, the guidance systems built into the kit - inertial and GPS systems - allow the glide bombs' trajectories to be adjusted during flight, so that the targets can be engaged with the precision normally associated with other, more expensive precision munitions. Given the range of glide bombs and the accuracy with which they can engage ground targets, these munitions can be launched from areas that are safe for aerial platforms, out of the range of enemy air defense systems.

## The threat posed by glide bombs

In the initial phases of the conflict in Ukraine, the Russian military failed to destroy the vast majority of Ukrainian medium- and long-range surface-to-air missile systems. This, coupled with Ukraine's constant resupply of man-portable air defense

systems, has posed a high risk to Russian air platforms designed to bomb targets close to the front line, as well as in more remote areas of Ukrainian territory. For this reason, by April 2022, the Russian military had limited aerial attempts to penetrate the enemy combat formation. In the Ukrainian conflict, the Russian Air Force is facing an enemy with a multitude of ground-based air defense systems that form a layered defense against aerial platforms. As I have mentioned, the Russian military has failed to destroy most of these air defense systems, in particular the Ukrainian S-300 and Buk-M1 medium- and long-range surface-to-air missile systems, respectively. As a consequence, Russian aircraft attempting to support by fire ground forces have to fly at low and very low altitudes when venturing close to the front line, but this makes them vulnerable to MANPAD-type systems and prevents them from effectively using unguided bombs.

The insufficiency of precision strikes has meant that the Russian Army's ground force support has been carried out with unguided projectiles, and therefore with very high risks for the aerial platforms engaged in launching them. This growing need for precision munitions prompted the development of the gliding kit - UMPK in January 2023. It is an inexpensive kit that can equip conventional aviation bombs with wings and guidance systems, allowing them to be deployed on fixed targets outside the range of Ukrainian air defense. The advent and use of glide bombs have practically brought the Russian Air Force "back to life", as it is now able to engage ground targets in the enemy's combat formation, without having to secure air superiority in advance or to venture by penetration inside the Ukrainian forces' combat system.

The UMPK gliding kit is the Russian version of the American-made JDAM (Joint Direct Attack Munition), more specifically the JDAM-ER (Extended Range) kit used by the Ukrainian army. It should be noted that, similar to the UMPK, the JDAM is a kit used to convert simple or standard unguided bombs into precision 'smart' munitions for use on ground targets, including in adverse weather conditions. With the addition of a new tail section containing an inertial navigation system and a GPS guidance unit, the JDAM kit improves the accuracy of general-purpose unguided bombs in all weather conditions. A version of the JDAM-ER kit used by the Ukrainian military is the one attached to the Mark 82 500-pound (230 kg) bombs

**Figure 1** **JDAM-ER** (Newsweek 2023)

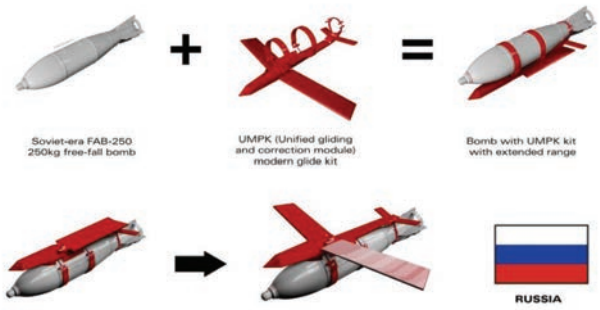



**Figure 2** **UMPK** (Al-Rifai 2024)

dropped from Su-27 aircraft to hit targets at ranges of 72 km with a circular error of up to 11 m. (Kushnikov 2023)

According to Ukrainian Air Force spokesman Yuriy Ihnat (Hardie 2023), the UMPK gliding kit allows bombs to engage targets at ranges of 43 miles. He said that this provides Russian Su-35S or Su-34 aircraft with the ability to strike fixed targets at ranges of up to 12-18 miles inside the Ukrainian forces' combat formation while remaining out of range for Ukrainian air defense systems, which usually stay farther from the front line for safety reasons. One response to this type of action has been to bring air defense systems closer to the front line, thus increasing their vulnerability to artillery strikes and Lancet loitering type munitions.

Today, the use of the new munitions is described by the Ukrainian side as an extreme threat (Vesti din Rusia 2025), with the Ukrainian armed forces having difficulties in intercepting or jamming them. Glide bombs are conventional air-launched munitions that have been equipped with wings and satellite-assisted navigation to extend their range and accuracy in engaging targets. They represent a cheaper targeting alternative to the ballistic and cruise missiles that Russian forces regularly launch over Ukraine. Glide bombs, weighing between 500 kg and 3000 kg (Peleschuk 2024), are available in large numbers to the Russian military, including from the Soviet era, and can be carried by aerial platforms to be launched from outside the air defense ranges of the Ukrainian forces.

If a 152 mm artillery shell contains 6.5 kg of explosive material, a small-sized glide bomb contains over 200 kg (Inwood and Kharchenko 2024). Striking the defensive positions of Ukrainian forces with such munitions makes it almost impossible to withstand them, regardless of the degree of cover and reinforcement for defensive positions. The availability of sufficient quantities, coupled with the possibility of launching them from a distance, allows the Russian forces to practically pummel and annihilate any defensive position, regardless of their level of prior fortification. Moreover, these glide bomb attacks allow the annihilation of Ukrainian defensive positions without the use of Russian infantry, which in itself constitutes a considerable advantage for any adversary.

Glide bombs have been used successfully by Russian forces mainly in attacks on fixed targets such as command posts, fortifications, or ammunition depots, but these munitions have also been used against the civilian population, striking urban centers in places such as Sumy, Kharkov, and Zaporozhe (Hodunova 2025). The psychological effect thus achieved and the potential for influencing the morale of Ukrainian troops cannot be ignored. The very high destructive power of aviation bombs converted into glide bombs is a deterrent for Ukrainian servicemen, since the absence or impossible recovery of the bodies for those killed deprives their families or relatives of the due compensation (Watling and Reynolds 2025, 16).

Another noteworthy aspect of the use of glide bombs is, in my view, the exploitation of the characteristics of these munitions, particularly their accuracy and destructive power, to hit Ukrainian artillery firing positions, thus practically integrating glide bombs into the counter-battery fire of the Russian forces. The "artillery hunting" drones usually have small explosive charges and ensure the target neutralizing effect, but glide bombs contain significantly larger explosive charges, which ensure the destructive effect of artillery systems.

The threat from glide bombs is all the greater for the Ukrainian side if we consider the use of these munitions in combination with other "conventional" attacks, with standard missiles or cruise missiles, creating an overload effect on the possibilities of air defense systems. One factor that made it more difficult to counter glide bomb attacks was the delays in aid from European partners and delays in deliveries of arms and ammunition for Ukrainian air defense by the United States (Di Mizio and Barrie 2024).

The significant increase in the number of glide bombs from 40,000 units in 2024 to an estimated 70,000 units in 2025 (Watling and Reynolds 2025, 7) has a direct impact on the number of casualties among Ukrainian troops in defensive positions while defending important objectives. The highly destructive power, characteristic of glide bombs, has led to the need to adapt the arrangement of defensive positions of Ukrainian maneuver forces in the sense that platoon or company strongholds include larger underground communication networks to reduce the risk of burying servicemen in the event of hitting trench sections with such glide bombs. The effects of the increased threat of these glide bombs have also been felt by the Ukrainian armed forces and structures operating within their range, which have had to take additional protective measures either by dispersal or by camouflage and concealment in relation to the enemy's observation capabilities.

The technical characteristics and the availability of glide bombs in sufficient quantities made it possible to exploit their effects in the actions of maneuver structures, and they came to be used even for fire support of assaults using squads or platoons (Watling and Reynolds 2025, 8). The identification of the defensive positions of the Ukrainian forces by successive assaults is followed by artillery, drone, and glide bomb strikes of various sizes.

I have presented below in tabular form the destructive possibilities of glide bombs of various sizes that are available to the Russian forces.
The effective use of glide bombs by Russian forces in destroying fortified positions of Ukrainian defenders in towns such as Avdiivka, has prompted some media analysts to question whether glide bombs are Russia's ultimate weapon or a sign of Ukraine's poor equipment - *"Glide bombs: Russia's 'ultimate weapon' or a sign of Ukraine's under-equipment?"* (Lefief 2024).

**TABLE NO. 1**
**Effects of aviation bombs used by the Russian Army**

| Bomb type | Lethal distance 100% | Probability of wounding 10% |
|---|---|---|
| FAB-100 | 7,75 m | 31 m |
| FAB-250 | 10,12 m | 40 m |
| FAB-500 | 12,75 m | 51 m |
| FAB-1500 | 18,78 m | 75 m |
| FAB-3000 | 24 m | 167 m |
| FAB-9000 | 35 m | 245 m |

**Source:** (Miler 2024)

## Ways to counter the glide bomb threat

The use of glide bombs in Ukraine has ensured that both sides in the conflict have been able to hit ground targets accurately, at long distances, while providing anti-aircraft safety for the aerial platforms destined to launch them. As for the Russian forces, the availability of generous stocks of aviation bombs has enabled the launch of increasing numbers of such glide bomb attacks, prompting the Ukrainian military and its allies to seek viable solutions to counter the threat.

This threat posed by glide bombs is recognized even at the alliance level (NATO 2025), as they are difficult to counter from an air defense point of view, due to the characteristics of the bomb (such as speed, thermal or acoustic signature) and the high volume of launches that can saturate air defense systems in the areas (or in the time frame) targeted by such attacks. Another aspect taken into account at the NATO level is the cost ratio in favor of glide bomb attacks, at the expense of the resources involved and consumed in air defense actions and in countering these munitions. As an additional element of the glide bombs' challenge, the aforementioned characteristics of glide bombs make some air defense assets ineffective in countering them. These include munitions using infra-red sensors such as the AIM-9 Sidewinder and FIM-92 Stinger missiles (Hodunova 2025).

The most practical methods to combat glide bomb attacks are, according to some experts (Hoehn and Courtney 2024) and Ukrainian officials, to combat aerial platforms intended to launch such attacks. Striking ground targets, represented by aircraft on the ground, by Ukrainian forces using both drones and Army Tactical Missile System (ATACMS) launched by High Mobility Artillery Rocket System (HIMARS), has proven to be the first such effective method of countering glide bomb attacks. Although it requires a longer period of time to produce effects, I may also mention here the reduction in the number of flights or sorties for carrier air platforms over time, by affecting any domain of the Russian aviation segment, as an effective method of reducing the number of glide bomb attacks.

Destroying aerial platforms, designed to drop glide bombs, in mid-flight would be a second effective method of countering glide bomb attacks. This effect can be achieved either by using air strike capabilities, such as the Advanced Medium-Range Air-to-Air Missiles (AMRAAM) carried by Ukrainian F-16s, or by having sufficient long-range air defense capabilities such as PATRIOT or SAMP/T (Peck 2024).

A third method of countering glide bomb attacks is through electronic warfare equipment. Jamming the GPS signal required by glide bomb guidance systems will cause ground target engagement to be based on secondary inertial systems, which will affect accuracy. The likely target hit errors increase in direct relation to the glide bomb flight distance without GPS assistance. An example of electronic warfare equipment, effective against glide bombs, seems to be the Lima system developed by the Night Watch team in Ukraine (Axe 2025). It works on several levels on navigation systems, using a combination of jamming, spoofing, and cyber-attacks on glide bomb GPS receivers, thus causing significant deviations from the intended targets, rendering glide bomb attacks ineffective.

Disrupting the supply chain of glide bombs by hitting production facilities, as well as their storage locations before they are loaded onto aerial platforms, is another effective method of countering glide bomb attacks. In 2024, several Ukrainian strikes, employing long-range drones, penetrated Russian air defenses and destroyed large munitions depots, including glide bomb depots located in the vicinity of airfields where carrier aircraft were stationed. One example is the attack and destruction of such a large munitions depot in Tikhoretsk (Al-Rifai 2024). To this end, the Ukrainian side also insisted on long-range munitions for HIMARS systems and the approval of the US administration to strike targets deep inside the Russian Federation.

Another method of countering glide bomb attacks is by destroying glide bombs in flight, using tactics proven effective against Russian Shahed 136 drones (Hambling 2025). These tactics are based on the placement of sensors and strike assets close to the front line in stand-off positions, aimed at detecting and intercepting glide bombs that are launched from enemy-occupied areas. The system integrates both artificial intelligence elements to increase the probability of success rate, and anti-aircraft guns or intercept drones to destroy glide bombs.

Regardless of which measures to counter glide bomb attacks are to prove their viability and effectiveness over time, the constant issue remains the need for combat forces to adapt to the new realities of the operational environment, a need that can reverberate in any domain. We are thus witnessing changes implemented by the armed forces of both warring parties, changes in the strategy applied in the conflict, changes in the doctrine for the use of land or air forces, changes in the way in which force structures are equipped and manned, changes in the way in which defensive positions are set up and occupied or assaulted, etc.

## Conclusions

The use of glide bombs to attack various ground targets and support military action in general is not new today. These means have been exploited in many other conflicts in the past, their origins having been traced back to the world wars of the last century. The novel aspect of the recurrent use of glide bombs in operations is the exploitation of the large numbers of these means, mainly due to the cost-effectiveness involved, to overwhelm the air defense systems of any adversary. The development and refinement of gliding kits, in conjunction with effective target-guidance systems, gives today a substantial advantage to Russian forces in the Ukrainian conflict, ensuring the possibility of employing aerial platforms in a new way - different from the way they were used at the outset of the conflict, without having to secure air supremacy or air superiority.

The effects of the mass use of glide bombs are both physical, such as the destruction of any defensive positions in the advancing direction of Russian forces, and psychological, which has a significant impact on the morale of the Ukrainian defenders and the civilian population affected by these attacks. The need to eliminate or diminish the devastating potential of glide bombs has prompted the Ukrainian army and its allies to seek solutions so that glide bombs do not become a real game changer in the Ukrainian conflict.

In this paper, I have focused on the defining characteristics of glide bombs and the impact of glide bomb attacks in order to emphasize their potential threat to the military operation as a whole. At the same time, I have considered various viable solutions analyzed, both at the level of the Ukrainian military and its allies, to effectively counter the threat posed by glide bombs. One thing remains certain: the need to adapt the force structures, applicable to both warring parties, to the new reality of the operational environment in the Ukrainian conflict.

## References

**Al-Rifai, Nizar.** 2024. *The Glide Bomb War: Evolving Aerial Combat Over the Ukrainian Battlefield.* https://offbeatresearch.com/2024/11/the-glide-bomb-war-tracking-the-proliferation-of-glide-bombs-in-ukraine/.

**Australian War Memorial.** 2025. *Fritz X Guided Missile.* https://www.awm.gov.au/collection/C152869.

**Axe, David.** 2025. *Ukraine Has Been Jamming Russian Glide Bombs. Now We Know How.* https://www.forbes.com/sites/davidaxe/2025/03/17/ukraine-has-been-jamming-russian-glide-bombs-now-we-know-how/.

**Di Mizio, Giorgio, and Douglas Barrie.** 2024. *Russian glide bombs add pressure on Ukraine's diminishing air defences.* https://www.iiss.org/online-analysis/military-balance/2024/03/russian-glide-bombs-add-pressure-on-ukraines-diminishing-air-defences/.

**Gheja, Victor.** 2023. *Rusia foloseste bombe planante de 1.500 kg in Ucraina: „Este echipata cu sistem de navigatie prin satelit".* https://www.aktual24.ro/rusia-foloseste-bombe-planante-de-1-500-kg-in-ucraina-este-echipata-cu-sistem-de-navigatie-prin-satelit/.

**Hambling, David**. 2025. *A Ukrainian Mystery Weapon Is Shooting Down Russian Glide Bombs.* https://www.forbes.com/sites/davidhambling/2025/02/13/a-ukrainian-mystery-weapon-is-shooting-down-russian-glide-bombs/.

**Hardie, John.** 2023. *Can Russia's New Guided Glide Bombs Help Blunt Ukraine's Counteroffensive?* https://www.fdd.org/analysis/2023/05/30/russias-new-guided-glide-bombs/.

**___.** 2024. *Photos offer insights on Russia's new UMPB D-30SN glide bomb.* https://www.longwarjournal.org/archives/2024/06/photos-offer-insights-on-russias-new-umpb-d-30sn-glide-bomb.php.

**Hodunova, Kateryna.** 2025. *Russia's primitive glide bombs are still outmatching Ukraine's air defenses, killing more civilians.* https://kyivindependent.com/russias-primitive-glide-bombs-are-still-outmatching-ukraines-air-defenses-killing-more-civilians-2/.

**Hoehn, John, and William Courtney**. 2024. *How Ukraine Can Defeat Russian Glide Bombs.* https://www.rand.org/pubs/commentary/2024/06/how-ukraine-can-defeat-russian-glide-bombs.html#:~:text=The%20most%20practical%20counter%20to,air%20capabilities%2C%20and%20electronic%20warfare.

**Inwood, Joe, and Tania Kharchenko.** 2024. *Russia's glide bombs devastating Ukraine's cities on the cheap.* https://www.bbc.com/news/articles/cz5drkr8l1ko.

**Kushnikov, Vadim.** 2023. *Ukrainian Su-27s are using JDAM-ER standoff bombs.* https://militarnyi.com/en/news/ukrainian-su-27s-are-using-jdam-er-standoff-bombs/.

**Lefief, Jean-Philippe.** 2024. *Glide bombs: Russia's 'ultimate weapon' or a sign of Ukraine's under-equipment?* https://www.lemonde.fr/en/international/article/2024/04/25/glide-bombs-russia-s-ultimate-weapon-or-a-sign-of-ukraine-s-under-equipment_6669544_4.html.

**Miler, Sergio.** 2024. *FAB 3000 Glide Bomb: Threat or Stunt?* https://wavellroom.com/2024/09/13/fab-3000-glide-bomb/.

**NATO**. 2025. *Harnessing Innovation to Counter Glide Bombs.* https://www.act.nato.int/article/harnessing-innovation-counter-glide-bombs/.

**Newsweek.** 2023. U.S. Winged JDAM Smart Bombs Operational in Ukraine—Air Force General. https://www.newsweek.com/us-winged-jdam-smart-bombs-ukraine-air-force-1786238.

**Okoko, Janet Mola, Scott Tunison, and Keith D. Walker.** 2023. *Varieties of Qualitative Research Methods.* Saskatoon: Springer Texts in Education.

**Peck, Michael**. 2024. *Glide Bombs: The Russian Wonder Weapon?* https://cepa.org/article/glide-bombs-the-russian-wonder-weapon/.

**Peleschuk, Dan**. 2024. *Key facts about Russia's highly destructive 'glide bombs'*. https://www.reuters.com/world/europe/russian-guided-bombs-wreaking-havoc-ukraine-2024-09-25/.

**Vesti din Rusia.** 2025. *Asia Times: Bombele de tip planor ale Rusiei au pus Ucraina în impas.* https://www.vestidinrusia.com/2023/04/25/asia-times-bombele-cu-planare-ale-rusiei-au-pus-ucraina-in-impas/.

**Watling, Jack, and Nick Reynolds.** 2025. *Tactical Developments During the Third Year of the Russo–Ukrainian War.* London: Royal United Services Institute.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Theoretical Concepts used in building Cyber Resilience

**Capt. cdr. Claudiu-Cosmin RADU***

*Command and Staff Faculty, "Carol I" National Defence University
PhD student in Intelligence and National Security
e-mail: radu.claudiu@unap.ro

## Abstract

In the context of intensifying cyber threats, cyberspace resilience has become a strategic priority for organizations, governments, and international alliances. Cyber scenarios, in their various forms, provide a controlled environment in which response capabilities to cybersecurity incidents can be tested, trained, and validated. The aim of this paper is to analyze how these scenarios contribute to the development of an organizational culture of resilience, allowing the identification of vulnerabilities, strengthening decision-making under pressure, and proactively adapting to new types of threats. The study explores current practices adopted at the European and international level, revealing how scenario-based exercises support strategic planning, training of technical and operational teams, and interinstitutional cooperation. Moreover, the direct benefits to organizational flexibility and post-incident recovery capacity are also analyzed. Finally, the article formulates a series of recommendations for integrating scenarios into the cyber risk management cycle, highlighting their value not only as training tools but also as fundamental elements in the security architecture of a modern organization.

**Keywords:**
cyber resilience; cyber scenarios; cyber exercises; wargaming; civil-military collaboration; planning; TTX exercises.

**Article info**
Received: 14 May 2025; Revised: 6 June 2025; Accepted: 11 June 2025; Available online: 27 June 2025

Citation: Radu, C.C. 2025. "Theoretical Concepts used in building Cyber Resilience". *Bulletin of "Carol I" National Defence University*, 14(2): 267-284. https://doi.org/10.53477/2284-9378-25-29

In a profoundly digitalized society, organizations face an increasingly diverse spectrum of cyber threats that target sensitive data and can severely disrupt the functioning of essential IT systems To deal with these challenges, it is imperative to adopt innovative resilience-building methods that ensure not only resilience to attacks but also rapid and efficient recovery. An accessible and effective solution in this regard is the use of cyber scenarios. These provide organizations with the opportunity to anticipate emerging threats and to build responses tailored to the specific nature of those threats. As the complexity and sophistication of cyberattacks intensify, traditional defence mechanisms become increasingly inadequate. At the same time, the growing number of interconnected devices expands the potential attack surface, exposing critical institutional networks to vulnerabilities that are progressively harder to control. In such circumstances, scenarios become essential tools for testing response capabilities, validating business continuity plans, and optimizing security architecture.

Amidst the profound transformations driven by accelerated digitalization, cyberspace has become a strategic domain, essential for the functioning of critical infrastructures, government services, economic activity, and social communication. The more societies have come to rely on information technologies, the more deeply vulnerable digital systems have become in the face of increasingly complex and hard-to-predict risks. From geopolitically motivated cyberattacks to ransomware campaigns that paralyze hospitals, public administrations, or civilian companies, cyber threats have diversified significantly and evolved into increasingly sophisticated and operationally coordinated forms. These attacks are often orchestrated by specialized groups, whether motivated by economic gain or strategic agendas, and benefit from advanced technical resources, hierarchical structures, and coordinated action methods at the transnational level. Against this backdrop, cyberspace has become a constant source of instability, vulnerability, and systemic risk, affecting critical infrastructures, supply chains, and essential systems of digital governance.

The concept of cyber resilience has gained significant importance in both national and international security strategies. Resilience is no longer seen merely as the capacity to recover from an incident, but rather as a proactive set of measures, competencies, and mechanisms that allow for the anticipation, absorption, adaptation, and systemic improvement of functions affected by disruptive events. According to the European Union Agency for Cybersecurity (ENISA), resilience can be associated with the capacity of cyber systems to withstand, respond to, and recover from an attack or malfunction, while ensuring the continuity of essential services.

One of the most effective methods for testing and improving resilience is the use of cyber scenarios. Based on these scenarios, complex, structured exercises are developed, grounded in either hypothetical situations or real-world case studies, simulating attacks, security breaches, or crisis situations. Through these scenarios, organizations can assess not only the response of technical teams but also managerial

capacity, internal and external communication, as well as decision-making processes under stress and informational uncertainty.

Cyber scenarios can take various forms. Some of the most widely used are Tabletop Exercises (TTX), which involve strategic discussions based on hypothetical scenarios and simulated situations. Others include Live-Fire Exercises (LFX), which simulate real attacks in a controlled environment. Cyber Wargaming tests tactical and operational capabilities in a competitive framework. In addition, Capture-the-Flag (CTF) competitions focus on identifying and exploiting vulnerabilities within a simulated environment. All of these formats contribute, in varying degrees depending on the purpose and structure of the exercise, to the development of an organizational culture oriented toward prevention, preparedness, and adaptability.

The importance of scenarios is highlighted by numerous international initiatives, such as the *Locked Shields* exercises organized by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) or the *European Cybersecurity Challenge* coordinated by ENISA, which emphasize interinstitutional cooperation, real-time response evaluation, and collective learning. Essentially, cyber scenarios enable a systemic approach to risk management by contributing to the identification of vulnerabilities, the testing of continuity plans, and the enhancement of resilience, not only technical but also organizational. Thus, they become not merely didactic or technical tools, but true laboratories of cybersecurity. Basically, the future is explored through the lens of cyber scenarios.

**Research methodology**

The primary aim of this research is to analyze the roles of cyber scenarios and exercises in strengthening and maintaining organizational resilience within cyberspace. The study is conducted within a qualitative, exploratory-analytical framework, specific to the field of cybersecurity, with a focus on documentary and contextual analysis.

The methodology is based on the study of specialized literature, the NATO and EU doctrinal framework, as well as relevant documents in the field of cybersecurity and cyber defence.

Using this methodological approach, the research has achieved the following primary objectives:

**1. Reviewing the specialized literature to clarify the theoretical concept of scenarios and cyber scenarios.** This stage provides the epistemological foundation of the paper and is based on academic and technical literature, as well as on validated institutional sources (ENISA, NIST, CCDCOE).

**2. The literature review on the functions and applicability of cyber scenarios** aims to demonstrate that they are not just didactic or operational tools, but essential mechanisms that can be integrated into the contemporary cybersecurity architecture and in the process of building organizational resilience. In support of this

demonstration, the analysis is complemented by benchmarking the most commonly used exercise formats: Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red/Blue Team Exercises and Capture-the-Flag (CTF), which are analyzed in terms of their role in developing cyber capabilities, theoretical and operational readiness, and developing an organizational culture oriented towards deterrence, adaptation and rapid response.

The research employs secondary qualitative methods to analyze data and information from open sources, studies, and specialized reports. This methodological choice is justified by the multidimensional nature of the subject, as well as by the objective of providing an integrative analytical framework with practical applicability across institutional, military, and civilian environments.

Multiple types of scenarios and exercises applied in national and international contexts were analyzed, with the goal of highlighting their impact on the development of cyber resilience. The analysis was guided by operational criteria, assessing the practical relevance of each exercise format and its alignment with institutional defence and response objectives. The inherent limitations of qualitative research, such as the lack of validation through quantitative empirical data, do not undermine the practical value of the conclusions, as the approach focuses on identifying best practices, lessons learned, and strategic directions for strengthening cybersecurity architecture through structured scenarios and exercises. Moreover, the adopted methodology aims to support the central argument that cyber scenarios and exercises are not merely training tools, but strategic components of cyber resilience that can directly enhance an organization's ability to prevent, respond to, and recover from emerging cyber threats.

## 1. Literature review on the theoretical concept of scenario

Scenarios should not be confused with forecasts or predictions of the future; they are hypothetical but plausible situations designed to test systems' reactions and to train personnel specialized in cyber defence and security. By their nature, scenarios provide a controlled framework in which crisis events can be simulated, enabling the evaluation of response capabilities, adaptability, and coordination among the actors involved. Furthermore, scenarios may serve as a valuable resource in the planning and decision-making process for military commanders, offering operational and strategic benchmarks based on lessons learned from previous exercises or wargames.

One of the core objectives of using scenarios is to reduce operational uncertainty and, implicitly, the number of unforeseen incidents. This has a direct impact on the level of stress and pressure placed on specialists who, through training, develop operational reflexes that can be triggered automatically in real-life situations. Thus, even if a cyber incident cannot be avoided, the ability to detect and respond to it in

minimal time represents a major strategic advantage. In this regard, **the effectiveness of scenarios** is measured not only by the fidelity of the simulation but also by their capacity to generate real changes in organizational behavior: reducing reaction times, increasing team cohesion, refining decision-making processes, and, not least, strengthening trust in one's own defence mechanisms. The more a scenario is adapted to the organization's specific context and rigorously constructed, the higher its formative yield, directly contributing to the enhancement of cyber resilience.

In recent years, an increasing number of studies have focused on exercises and wargames from a military perspective. As outlined in previous sections, the purpose of this article is to analyze the importance of scenarios in improving cybersecurity. This approach may be both military and civilian. Moreover, joint exercises conducted by member states of alliances and international organizations, along with partnerships between civilian and military structures, directly contribute to strengthening cyber resilience. The synergistic effect arises from training specialists in various operational contexts, both simulated and realistic. Although they may seem abstract at first glance, these scenarios significantly reduce uncertainties, providing essential support in the institutional preparedness and response process. In addition, they shorten the response time in the event that hypothetical situations materialize.

The scenario, composed of multiple hypotheses, is based on a presumed attack that tests operational and legal procedures, as well as information exchange protocols with alliance partners. Participants collaborate to identify the threat as quickly as possible and to limit its impact on the national systems of each state involved. It is important to emphasize the synergy of collaboration between military and civilian institutions. Moreover, joint exercises among allied states and cooperation between civil and military institutions are essential for optimizing resilience in the face of cyber threats. Cyberattack scenarios should test not only operational but also legal procedures (Nucă 2024), ensuring that all involved parties can react efficiently and in a coordinated manner. These exercises contribute to specialist training, developing both practical and theoretical skills essential for managing exceptional situations in cyberspace. Furthermore, international collaboration within these exercises helps build trust among states and establish common standards for responding to cyber threats. Additionally, cybersecurity and cyber governance are fundamental elements for ensuring the sustainable functioning and durable development of any organization or society (Popa 2015, 22).

If we strictly refer to the similarity of cyber scenarios with military scenarios, some experts argue that the scenario is closely linked to the concept of a contingency plan, as it involves identifying and establishing a specific course of action applicable under well-defined circumstances (Petrescu 2017, 62). In planning practice, commanders prioritize identifying the most probable threat or the most dangerous course of action by the adversary, as well as formulating an appropriate response to the respective situation. The efficiency of the decision-making process is enhanced by

using scenarios within wargames, allowing planning efforts to focus on formulating operational solutions adapted to various hypotheses regarding the evolution of tactical or strategic situations. Thus, the risk of being surprised by the enemy is reduced through a clearer anticipation of maneuver possibilities and alternative courses of action (Joint Chiefs of Staff 2020, III-4).

Currently, the scenario has become an essential tool in the planning process of military actions, offering a coherent and structured methodology for analyzing possible future situations. This approach helps clarify the inherent uncertainties of the operational environment and supports decision-making by outlining plausible perspectives on the evolution of the situation (Schoemaker 1995). A complete scenario should include a description of the initial state, the articulation of a possible or desired end state, and a logical sequence of events leading from the current to the final state, provided that certain determining factors are met (Van der Heijden 2005, 152). In order to be effective, a scenario must be sufficiently coherent, transparent, and logical, so that it can be analyzed and evaluated in relation to the formulated hypotheses (Godet 2006).

It is essential to emphasize that scenarios are not intended to eliminate uncertainty completely, nor to predict future developments with precision. They do not forecast the future, but delineate a reference framework that defines its boundaries, thereby enabling a more nuanced understanding of potential operational developments (Wright and Goodwin 2009). Scenarios have been defined over time in different ways and from different perspectives. However, one of the most well-known scenario theorists, Philip van Notten, defines a scenario as *"a coherent and comprehensive description of an alternative and hypothetical future situation, reflecting different perspectives on the past, present and possible future developments, and serving as a basis for further decisions and actions"* (van Notten 2005, 20). In his paper, van Notten synthesizes several academic and applied perspectives on scenarios, highlighting that the term has at least four major meanings: as a sensitivity analysis tool, a contingency plan, a strategic decision-making instrument, and an exploratory method of learning and anticipation. The latter meaning is central in contemporary research and is supported by an emerging consensus in the specialized literature: scenarios are not predictions but plausible and structured representations of possible alternative futures (van Notten 2005, 18).

The practical relevance of scenarios derives not only from their descriptive value but also from their ability to influence decisions and stimulate strategic thinking. Thus, Postma emphasizes internal logic by stating that *"scenarios are descriptions of coherent pictures of future events and situations"* (Postma and Vijverberg 1995), while Fahey and Randall emphasize probability: *"scenarios are plausible descriptive narratives of alternative projections of a specific part of the future"* (Fahey and Randall 1998). Other authors, such as Van Asselt and Rotmans, propose an integrative view, which includes not only the future, but also reinterpretations of the past and

the present: *"scenarios are narrative descriptions of alternative images of the future, constructed based on mental and conceptual models that reflect different perspectives on the past, present and future"* (Rotmans 1998).

Scenarios are analytical constructs designed to outline a variety of future conditions, including opportunities, threats, and potential obstacles that can significantly influence the achievement of desired objectives. They guide the interpretation and approach to uncertain situations while providing a reference framework for decision-making and the selection of courses of action. A defining attribute of scenarios is their conceptual flexibility, which allows for the integration of a wide range of development directions. Each direction is based on a specific set of values associated with determining factors, whose interactions give the scenario operational coherence and relevance. The constituent elements of the scenario are interconnected through logical and functional relationships, built on methods, principles, procedures, and rules that together form an integrated normative system. This system supports a structured deployment of actions and contributes to shaping a strategic response adapted to the complexity of the analyzed environment.
Scenario definitions converge toward a complex and multidimensional vision, in which a scenario is simultaneously: a logical narrative about possibilities, a decision-making and learning tool, a framework for strategy testing, and a conceptual map of future uncertainties and trends. This integrated approach places the scenario at the center of the strategic resilience and anticipatory planning process in the face of systemic uncertainties.

In the context of cybersecurity, regardless of whether scenarios are based on real, fictional, or combined foundations, they must meet a set of essential requirements. First, they must be credible, meaning they should project possible situations in cyberspace, taking into account the complexity of digital infrastructure, informational interdependencies, and potential attack vectors. A realistic scenario enables a realistic assessment of cybersecurity capabilities and response procedures without altering the relevant parameters of the operational environment or the nature of the simulated threats. An essential condition directly linked to realism is the objectivity of the information used in constructing the scenario. It is crucial that the cyber environment, including triggering events, involved actors, exploited vulnerabilities, and institutional responses, be described clearly and precisely. The presentation should be free from ambiguity, redundancy, or excessive detail, as this could have a negative impact on understanding or practical application. However, the cyber scenario must be complete, objective, and well-structured, which means that all defensive and response skills must be integrated into a clear operational framework. This involves modelling both the *technical* aspects (networks, systems, data flows) as well as the *organizational and legal* aspects (decision flows, communication, and interinstitutional collaboration following existing legislation).

Another essential requirement is flexibility. The scenario must allow for real or simulated testing, so as to faithfully reflect the dynamics of cyber incidents and

permit the adjustment of the event sequence based on observed reactions. To determine the strengths and weaknesses of the given cyber system, validation can be carried out through practical exercises or digital modeling.

Finally, an essential characteristic is coherence. The scenario must be built on a clear and logical line, describing the operational situation fluently and coherently, and enabling the actors involved in crisis management and decision-making to integrate effectively. It should address the description of the situation in a structured and articulate manner, with information presented in close correlation, efficiently placing the target structure within the operational environment necessary for achieving objectives (Petrescu 2017, 66). Such a structure ensures the scenario's relevance for enhancing responsiveness, adaptability, and resilience to emerging cyber threats.

Scenarios are fundamental methodological tools used to explore uncertainties about future developments. As defined by Kosow and Gaßner, a scenario is *"a plausible description of a future situation, including development paths that could lead to that situation"* (Kosow and Gaßner 2008). Scenarios should not be confused with predictions or forecasts. They are hypothetical constructs intended to provide a framework for systematic reflection on the determinants and interdependencies that shape possible futures.

According to the same authors, scenarios serve several essential functions (Kosow and Gaßner 2008).

a) Exploring existing knowledge and identifying information gaps;
b) Facilitating communication between different actors involved in the decision-making process;
c) Formulating strategic objectives under uncertainty;
d) Support planning and decision-making by anticipating possible changes and challenges.

The practical utility of cyber scenarios manifests across multiple dimensions, most notably in the support they offer for decision-making, the training of specialized forces, and the testing of interinstitutional collaboration procedures. By simulating complex incidents, scenarios enable decision-makers to anticipate adversarial behavior patterns, identify critical points in IT infrastructure, and rapidly adjust cyber incident response strategies based on threat evolution.

In terms of professional training, scenarios significantly contribute to the development of tactical and strategic skills among personnel in cybersecurity structures. Through controlled exposure to crisis situations, specialists learn to react effectively under pressure, manage contradictory information flows, and collaborate in real-time with internal and international experts. Additionally, scenarios foster critical thinking, anticipatory analysis skills, and an understanding of the interdependencies between components of a complex digital ecosystem.

At the institutional level, the implementation of scenarios facilitates the harmonization of doctrines and action protocols between military, civilian, public, and private structures. Cyber scenario-based exercises provide an effective platform for testing interoperability, verifying the compatibility of legal procedures, and identifying gaps in alerting, communication, and response mechanisms. Thus, scenarios become key tools in strengthening cyber resilience at both national and international levels within alliances.

The importance of using scenarios becomes especially evident in domains characterized by high uncertainty, where rapid or unforeseen changes can have major impacts on security, the economy, or the social environment (Kosow and Gaßner 2008). Furthermore, in a strategic environment marked by uncertainties and asymmetric and hybrid threats, an organization's ability to effectively integrate lessons learned from scenarios is essential for the continuous improvement of its security architecture. Therefore, scenarios should not be limited to isolated exercises but should be integrated as elements of a complex cycle of planning, learning, adjustment, and refinement of cyber defence.

## 2. Cyber scenarios - fundamental elements in cyber exercises

A cyber scenario can be interesting, unique, and specifically designed to address weaknesses or ambiguities in a *cyber incident response plan*. Moreover, such a scenario may constitute an intentional stress test for systems considered critical or those ensuring institutions' cybersecurity or even national security. The goal is to verify functionality under normal conditions and evaluate how the system reacts when deliberately pushed to its operational limits. Only in this way can vulnerabilities be identified and strengthened before being exploited in a real attack. In this process, the freedom to analyze even the most unlikely scenarios is key to an efficient and adaptive anticipation process. What happens if an attacker discovers a technical vulnerability and combines it with human error? Or if a seemingly minor breach opens the door to a series of incidents? Significant past cases have shown that extreme events, considered *pure bad luck* or *theoretically impossible*, often materialize in the cyber world. Through simulated exercises, organizations not only anticipate failures but also rehearse their responses. Each scenario is a lesson that transforms today's vulnerabilities into tomorrow's resilience.

Identifying these gaps is critical for enhancing our understanding of how scenario planning can be effectively incorporated into cyber resilience strategies. This integration ultimately leads to a stronger defence against evolving threats. Addressing these gaps will not only enhance theoretical frameworks but also offer practical insights for organizations looking to efficiently implement scenario planning in their cybersecurity practices.

Cybersecurity scenarios are essential tools for anticipating, modeling, and analyzing risks associated with the digital environment. They aid in understanding vulnerabilities and provide a methodological foundation for developing strategic and operational training exercises. As cyber threats have become more complex, the need to standardize various forms of training and testing has become increasingly apparent. Today, several types of cyber exercises are recognized, each adapted to different risks and training needs. These include Cyber Wargaming, Tabletop Exercises (TTX), Live-Fire Exercises (LFX), Red Team/Blue Team Exercises, Cyber Range Exercises, and Capture the Flag (CTF) Exercises, among others.

*Cyber Wargaming* is an analytical exercise akin to operational simulations or *tabletop* exercises, designed to replicate the dynamics of cyber conflicts in a controlled environment. The concept has its roots in military tradition, where wargames were used to train commanders and test battle strategies. As cyber threats have evolved and become more sophisticated, military methodologies have been adapted to the digital landscape. This adaptation allows for the assessment of an organization's security posture, decision-making processes, and defence strategies against cyberattacks. The connection between military wargaming and cyber wargaming highlights the importance of a structured and rigorous approach to modern cybersecurity. By conducting these exercises, organizations can anticipate potential surprises, identify hidden vulnerabilities, and strengthen their incident response procedures. At the same time, using its multidimensional approach - technological, procedural, and human - Cyber Wargaming provides an integrated framework for testing and optimizing security mechanisms under simulated crisis conditions. This approach allows not only the detection of technical or organizational weaknesses, but also the training of decision-makers and operational staff to respond effectively under pressure, in tense contexts or sophisticated attacks.

The essential purpose of cyber wargaming is to evaluate an organization's preparedness for major cyber incidents, test response capabilities, improve decision-making processes, and strengthen overall resilience to emerging cyber threats. By simulating conflicts in a safe environment, cyber wargaming contributes to developing more effective security policies, reducing reaction times during crises, and reinforcing interdepartmental cooperation within organizations.

This methodology is an essential tool for any organization looking to sustainably enhance its cybersecurity posture and improve its ability to manage attacks in a dynamic and adversarial digital environment. The use of wargames in the cyber domain still requires further development to realize its full potential. While many countries' armed forces recognize the implications of cyber threats for national security and regularly conduct cyber wargames at the national level or in collaboration with allies, the private and civilian sectors are still in the early stages of adopting these practices. Cyber wargames differ from traditional cybersecurity measures such as technical assessments, penetration tests, or vulnerability scans,

although they can be integrated when necessary. Beyond these conventional methods, cyber wargames offer a comprehensive evaluation of an organization's cybersecurity strategy by realistically simulating a cyber conflict. These exercises prepare both civilian and military organizations to make rapid decisions in unforeseen situations, such as shutting down parts of a network to contain damage. Cyber wargames thus contribute not only to the identification of technical vulnerabilities but also to the overall assessment of defence strategies, response mechanisms, professional skills, and resilience to a cyberattack. Designing and conducting controlled cyber warfare is a complex process that requires the involvement of experienced professionals and the use of state-of-the-art technologies. Since the goal of a cyber wargame is to provide participants with a near-real-time experience, scenario planners need to be familiar with both recent attack techniques and up-to-date defence methods.

Any organization, company, or institution can conduct independent wargames if it has the necessary technical infrastructure and qualified personnel. If these resources are lacking, it is advisable to outsource to specialized experts. The first step in planning and organizing a cyber war game is to clarify the scope and objectives. The scope can range from testing isolated tactics to operational or strategic assessment of the organization's cybersecurity system. The duration of the exercise, the level of participants, and the degree of complexity are determined according to the objectives and expectations initially defined. Conducting exercises in real environments carries additional risks, which is why it is recommended to use a Cyber Range platform. This solution allows for a realistic simulation of the organization's digital environments while minimizing the risk of interfering with actual operations systems and providing a learning experience under conditions close to reality (Abbas 2024).

By simulating near-realistic cyber incidents, Cyber Wargaming enables organizations to detect weaknesses, validate the effectiveness of security policies, update operational procedures, and prepare a coordinated response in critical situations. It also supports the development of an integrated cyber strategy by combining technical, procedural, and human elements to prevent costly surprises and manage emerging threats more effectively.

Another type of exercise using customized cyber scenarios for training is the Cyber Tabletop Exercise (TTX). This involves an interactive role-play simulation in which participants respond to hypothetical situations developed and presented by one or more scenario facilitators. Typically, they assume their actual roles within the organization, but depending on the exercise's needs, they may also play other roles to cover critical missing functions. Facilitators or scenario coordinators gradually introduce narrative elements that, although seemingly trivial at first, often conceal significant issues or systemic dysfunction indicators. Intentionally, contradictory information may be inserted to test the team's ability to critically analyze, prioritize risks, and maintain decision-making coherence in uncertain situations. This type of exercise is designed to support organizations in analyzing risk scenarios and

preparing for potential cyber threats. Being relatively easy to implement, these exercises provide an efficient and flexible tool for evaluating cybersecurity (Center for Internet Security 2025). Unlike operational exercises, a TTX does not aim to achieve perfect individual performance but focuses on practicing cooperation, identifying procedural vulnerabilities, and strengthening collective response capacity under normal conditions, when there is time to correct deficiencies. In a real incident, this time is no longer available, making such exercises essential for effective team preparation in a controlled yet realistic and challenging environment. Besides its formative value, this type of exercise is an effective and convenient tool for rapidly testing an organization's capacity to respond to cybersecurity incidents according to its own plans and procedures. Since there is no time to correct internal deficiencies during a real incident, such exercises become essential for team preparedness in a controlled but demanding environment. Furthermore, team coordination can no longer be optimized, which is why these exercises are essential in peacetime (Cybersecurity and Infrastructure Security Agency 2025).

*Live Fire Exercise* (LFX) is an advanced form of cybersecurity training in which participants react in real time to simulated attacks, conducted in a highly realistic, controlled technical environment. The largest and most sophisticated demonstration of this type of exercise is *Locked Shields*, organized annually by the NATO Centre of Excellence for Cyber Defence Cooperation, which brings together hundreds of experts from member and partner states. The purpose of this exercise is to test, in a simulated but operationally realistic environment, the security and defence capabilities of IT infrastructures and critical systems against highly complex cyberattacks. It also aims to strengthen the practical training of cybersecurity professionals by involving them in real-time activities within broad, interinstitutional, and multidisciplinary teams. The scenario is complex, designed to train participants in protecting governmental, military, and national critical infrastructures from multiple cyberattacks. Among the simulated infrastructures are banking systems, water, electricity, and natural gas distribution networks, satellite communication systems, and 5G networks (Ministry of National Defense 2023).

The exercise is structured on the Red Team vs. Blue Team model, where rapid reaction teams from NATO member states and partner countries are tasked with defending, in real-time, a fictional country subjected to a large-scale cyberattack. In addition to the purely technical and operational components, the exercise includes essential aspects of strategic decision-making, legal elements, public communication, and interinstitutional coordination. Thus, Locked Shields plays a vital role in refining operational competencies and strengthening international cooperation mechanisms in the cyber domain (The NATO Cooperative Cyber Defence Centre of Excellence 2022). It also provides an optimal framework for testing and refining response procedures to cyber incidents under intensely simulated crisis conditions, allowing for comparative performance evaluations of participating teams. The scenario

realistically and pragmatically reflects the complexity of modern cyber defence and the need for coordinated, integrated, and well-organized allied responses.
A distinctive element of the Locked Shields exercise is its holistic nature and performance-oriented approach. Furthermore, it provides a platform for testing defence procedures, interinstitutional collaboration, and developing innovative solutions for military, civilian, and academic environments. Participating teams were challenged to operate outside their professional comfort zones through surprise technical scenarios. In addition to strengthening their own capabilities, participants directly contribute to enhancing the content of the Locked Shields exercise through applied feedback on legal, strategic communication, and operational components.

The significance of this annual exercise lies not only in its technical complexity but also in the emphasis placed on transnational and multidisciplinary collaboration, the simultaneous training of experts from sectors such as defence, industry, and academia, and continuous adaptation to emerging technological challenges. Locked Shields demonstrates that effective preparation for cyber warfare requires a realistic, integrative, and anticipatory approach in which complex scenarios, interoperability, and strategic analysis are as crucial as protecting digital infrastructure itself (The NATO Cooperative Cyber Defence Centre of Excellence 2025). Moreover, multinational cyber exercises hold a central place in the strategic architecture for enhancing allied cooperation and promoting the exchange of best practices in cybersecurity. They provide a valuable operational framework in which allies can test, in a simulated but realistic environment, the interoperability and effectiveness of shared procedures, thereby increasing collective response capacity to real incidents. Additionally, by integrating civilian entities such as universities, research institutes, and private sector companies, these exercises help expand cyber defence capabilities beyond the strictly military domain. This civil-military cooperation enhances adaptability to emerging technological challenges and fosters a comprehensive approach to cyber risks based on complementary resources and competencies. In a global environment characterized by technological interdependencies and increasing digital vulnerabilities, such initiatives are indispensable for maintaining strategic superiority in cyberspace. They not only strengthen the national capacities of each member state but also lay the foundation for a coherent, agile, and effective collective defence. Furthermore, through their anticipatory and deterrent nature, these exercises contribute to reinforcing NATO's defensive posture, enabling coordinated responses to emerging threats and robust protection of critical infrastructures across the Euro-Atlantic area.

According to the definition provided by the National Institute of Standards and Technology (NIST) and cited by several experts, a *Cyber Range* can be *"an interactive, simulated representation of an organization's networks, systems, applications, and tools connected to an environment that simulates the real internet. They provide a safe and legal space for acquiring practical cyber skills, developing IT products, and testing*

*security posture*" (Chouliaras, Kittes, et al. 2021). The scenario is identified as one of the central pillars of a modern cyber range exercise. It plays a crucial role in shaping the exercises and generating relevant situations. Scenarios enable the introduction of realistic events with varying network typologies, automated user behaviors, and simulated attacks, contributing to the realism and complexity of the exercise. The purpose may vary, with the main objectives being (Chouliaras, Kittes, et al. 2021):

- *Research* - testing tools, methods, and components.
- *Education and training* - developing practical skills in cybersecurity.
- *Exercises and competitions* - running simulations, *Capture the Flag*, *Red vs. Blue Team,* or *Crisis Management Exercises*.

Unlike the other types of exercises, *Capture-the-Flag (CTF)* is a competitive cybersecurity exercise in which participants must identify and exploit cyber vulnerabilities to locate and extract a specific target, called a *flag*, usually represented by a hidden data fragment. These exercises simulate realistic attack and defence conditions, involving activities such as network analysis, reverse engineering, cryptography, or digital forensics (Rochford 2024). The main goals of these exercises are the following: on the one hand, they contribute significantly to the development of the technical and strategic skills of the participants, especially among talented young people or professional teams; on the other hand, they promote cybersecurity education and facilitate the formation of collaborative networks between organizations, institutions and experts from different fields. In particular, the "Attack-Defence" format is valuable for professional training, as it simulates real-life conditions in which teams must simultaneously defend their systems and attack the adversary's infrastructure (European Union Agency for Cybersecurity 2021). By their competitive nature, this type of exercise provides a dynamic training framework (Rochford 2024) for:

a) Modeling cyber threats;
b) Threat hunting;
c) Risk analysis;
d) Incident response;
e) Data collection;
f) Detection effectiveness;
g) Forensic evidence collection;
h) Critical Infrastructure Protection.

Regarding the role of the scenario in a CTF exercise, we could say it is essential for creating a realistic and coherent framework in which participants can test their knowledge and responses to cyber incidents. Scenarios may be inspired by real attacks or artificially constructed, but must be relevant, stimulating, and tailored to the participants' level. The scenario determines the nature of the challenges, tactical objectives, technologies used, and the complexity of the exercise. Thus, the scenario functions as the central element of the exercise, providing coherence in training within an operational context. CTFs are considered effective tools both for individual

training and for operational preparation of teams responsible for cybersecurity, depending on the chosen format.

The types of exercises presented above demonstrate how the practice of cyber wargaming is used in various contexts and sectors, both military and civilian, to improve defence capabilities, raise awareness, and build resilience against increasingly sophisticated and persistent cyber threats. Moreover, they can serve as essential tools for preparing and testing defence capabilities against cyberattacks. These exercises simulate realistic attack scenarios, allowing participants to develop practical skills, enhance incident response strategies, and strengthen organizational resilience to cyberattacks.

## Conclusions

Cyber resilience can no longer be conceived outside of dynamic and proactive preparedness mechanisms, where cyber scenarios play a fundamental role. In a digital landscape characterized by uncertainty, persistent aggression, and technological complexity, an organization's ability to respond effectively to incidents depends on the maturity with which it periodically tests and validates its own defence capabilities. Cyber scenarios have proven to be among the most effective tools for achieving this objective.

Scenarios, due to their simulated nature, allow for the replication of real or hypothetical contexts that are customized to fit the specific needs of an organization, the types of infrastructures it manages, and the expected level of threats. The scenarios created during cyber exercises - whether they are tabletop exercises (TTXs) focused on strategic decision-making or live-fire exercises (LFXs) that mimic real-time attacks - foster an accelerated learning environment. This enables teams to gain a better understanding of the strengths and weaknesses of their systems. Additionally, scenarios promote integrated learning, both technical and organizational, by bringing together IT experts, decision-makers, legal specialists, and security system managers in a collaborative setting. Another major advantage is the scenarios' capacity to support a collaborative approach to resilience. International exercises, such as Locked Shields or the International Cybersecurity Challenge, emphasize cross-border cooperation and the testing of interoperability mechanisms among agencies, states, and organizations. This collaborative character generates essential synergies for rapid and coordinated responses in the event of large-scale cyberattacks. At the same time, scenarios contribute to the standardization of best practices and the strengthening of the regulatory framework in the field of cybersecurity. In terms of educational dimension, CTFs and applied exercises conducted on cyber ranges are essential tools for training the new generation of experts. They allow not only the testing of technical knowledge but also the development of transversal competencies such as critical thinking, adaptability, and crisis management skills during critical

moments. The integration of these formats into national training programs and European initiatives like the Digital Skills Agenda (Misheva 2021) is a necessary step in strengthening the collective defence capability.

However, the practice of devising scenarios does have its limits. In the absence of a well-defined methodological framework, they can become formal, repetitive activities with little impact on learning processes. Additionally, scenarios not adapted to organizational specifics risk generating false results or creating a false sense of security. Therefore, the design and evaluation of exercises must be conducted by professionals using tested methodologies, such as those proposed by ENISA, NIST, or CCDCOE.

Another important aspect is the integration of scenario results into security policies and strategies. Lessons learned must be documented, analyzed, and transformed into concrete measures to strengthen the defence posture. This integration requires a formalized feedback process and an organizational culture open to continuous learning. Only in this way do scenarios become true governance tools in cybersecurity.

Cyber scenarios are more than simple simulation exercises; they constitute a complex framework for training, evaluation, collaboration, and transformation. When implemented strategically, with rigor and vision, they can become the backbone of resilience-building efforts in the digital domain. In a world where cyberattacks are no longer a possibility but a statistical certainty, investing in such tools is not a luxury but an imperative necessity for digital survival and informational sovereignty.

All these types of cyber exercises or simulations mentioned in this study are essential methods of operational training, contributing to the development of the response capacity to real cyberattacks. At the same time, they offer a controlled framework for testing offensive tactics to evaluate defensive capability and specific preparedness. Held annually or even multi-annually, these exercises bring together member and partner states in joint scenarios, becoming not only a means of enhancing interoperability but also a modern form of active deterrence in a climate marked by persistent and asymmetric cyber threats.

## References

**Abbas, Nasim**. 2024. „Cyber Wargames and Cyber Security." *Privia Security* pp. 3–8.

**Center for Internet Security.** 2025. *Tabletop Exercises (TTX).* https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx.

**Chouliaras, Nestoras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag.** 2021. "Cyber Ranges and TestBeds for Education, Training, and Research." *Applied Sciences* 11 (4): 1809. https://doi.org/10.3390/app11041809.

**Chouliaras, Nestoras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag.** 2021. "Cyber Ranges and TestBeds for Education, Training, and Research." *Applied Sciences* 11 (4): 1809. https://doi.org/10.3390/app11041809.

**Cybersecurity and Infrastructure Security Agency.** 2025. *CISA Tabletop Exercise Packages.* https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.

**___.** 2025. „Cybersecurity Tabletop Exercise Tips ." https://www.cisa.gov/sites/default/files/publications/Cybersecurity-Tabletop-Exercise-Tips_508c.pdf.

**European Union Agency for Cybersecurity.** 2021. *ENISA Threat Landscape 2021.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

**Fahey, Liam, and Robert M. Randall.** 1998. "What is Scenario Learning?" *Learning from the Future* pp. 3–21.

**Godet, Michel.** 2006. „Creating Futures: Scenario Planning as a Strategic Management Tool." *Economica* 39–45.

**Joint Chiefs of Staff.** 2020. *JP 5-0, Joint Planning.* https://irp.fas.org/doddir/dod/jp5_0.pdf.

**Kosow, Hannah, and Robert Gaßner.** 2008. *Methoden der Zukunfts- und Szenarioanalyse: Überblick, Bewertung und Auswahlkriterien.* research report, Bonn: Deutsches Institut für Entwicklungspolitik gGmbH.

**Ministry of National Defense.** 2023. *Specialiști din MApN, la exercițiul de apărare cibernetică Locked Shields 2023.* https://www.mapn.ro/cpresa/17900_Specialiști-din-MApN,-la-exercițiul-de-aparare-cibernetica-Locked-Shields-2023.

**Misheva, Galina.** 2021. *European Skills Agenda.* https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/european-skills-agenda.

**Nucă, Nicoleta.** 2024. *Aspecte ligislative privind războiul cibernetic sau cyberwarfare. Efectele și răspunderea penală.* https://www.juridice.ro/733058/aspecte-legislative-privind-razboiul-cibernetic-sau-cyberwarfare-efectele-si-raspunderea-penala.html.

**Petrescu, Dan Lucian.** 2017. *Modele conceptuale avansate pentru proiectarea și realizarea scenariilor militare în contextul mediului operațional de tip hibrid.* București: Universitatea Națională De Apărare „Carol I" .

**Popa, Iulian Florentin.** 2015. *Securitatea și guvernanța spațiului cibernetic contemporan.* Cluj-Napoca: Universitatea Babeș-Bolyai .

**Postma, Theodorus J.B.M., and A. M.M. Vijverberg.** 1995. "Toekomstverkenning met scenario's. Een hulpmiddel bij de bepaling van de strategische koers van een organisatie." *Bedrijfskunde: Tijdschrift voor Modern Management* 67 (2): 13-20.

**Rochford, Oliver.** 2024. *What is Capture the Flag in Cybersecurity? + Effective Exercises.* https://www.securonix.com/blog/capture-the-flag-in-cybersecurity/.

**Rotmans, Jan.** 1998. "Methods for IA: The Challenges and Opportunities Ahead." *Environmental Modelling and Assessment* 3 (3): 155–179.

**Schoemaker, Paul J.H.** 1995. „Scenario Planning: A Tool for Strategic Thinking." *MIT Sloan Management Review* 36 (2): 25–40.

**The NATO Cooperative Cyber Defence Centre of Excellence.** 2022. *Locked Shields.* https://ccdcoe.org/locked-shields/.

**___.** 2025. *NATO CCDCOE expands cyber defence cooperation ahead of the worlds largest live-fire exercise.* https://www.ccdcoe.org/news/2025/nato-ccdcoe-expands-cyber-defence-cooperation-ahead-of-the-worlds-largest-live-fire-exercise/.

**Van der Heijden, Kees.** 2005. *Scenarios: The Art of Strategic Conversation.* 2nd ed. New York: John Wiley & Sons.

**van Notten, Philip W. F.** 2005. „Writing on the wall : scenario development in times of discontinuity." Amsterdam: Thela Thesis & Dissertation. van Notten, P. W. F., Writing on the wall: scenario development in times of discontinuity. [Doctoral Thesis, Maastricht University], Thela Thesis & Dissertation.com, Amsterdam, 2005, pag. 20. https://doi.org/10.26481/dis.20050408pn.

**Wright, George , and Paul Goodwin.** 2009. "Decision Making and Planning Under Low Levels of Predictability: Enhancing the Scenario Method." *International Journal of Forecasting* 25 (4): 813–825. doi:10.1016/j.ijforecast.2009.05.019.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Decision-making Pragmatism in the Context of Hybrid-type Aggression

**Captain Diana-Elena CHIRILĂ***

*Training and doctrine directorate
e-mail: chirila_diana92@yahoo.com

## Abstract

Decision-making pragmatism plays a crucial role in managing hybrid aggression, a complex type of conflict that combines conventional techniques with cyberattacks, information manipulation, and economic pressure. In the face of such a threat, leaders must make swift and flexible decisions, constantly adapting to rapidly changing circumstances. Decision-making pragmatism involves using innovative and effective solutions that integrate technology, informational resources, and collaboration between civilian and military authorities. International cooperation and legislative adaptation are also essential in countering the effects of this type of conflict, given global interdependence. The pragmatic approach focuses on anticipating and responding quickly to unpredictable threats, thereby strengthening both national and international resilience. The conflict in Ukraine serves as a relevant example of the application of these principles, demonstrating the importance of pragmatism in effectively responding to hybrid aggression and contemporary challenges.

**Keywords:**

decision-making pragmatism; hybrid aggression; modern conflicts; cybersecurity; information manipulation; technology and warfare; international cooperation; national resilience.

**Article info**
Received: 6 May 2025; Revised: 2 June 2025; Accepted: 6 June 2025; Available online: 27 June 2025

Citation: Chirilă, D.E. 2025. "Decision-making Pragmatism in the Context of Hybrid-type Aggression". *Bulletin of "Carol I" National Defence University*, 14(2): 285-295. https://doi.org/10.53477/2284-9378-25-30

In recent decades, amid the rapid evolution of information technologies, globalisation, and changes in geopolitical structures, modern conflicts have become increasingly complex, and their nature has evolved considerably. As a result, conventional warfare as we knew it in the past has given way to much more sophisticated forms of aggression, which go beyond direct confrontations between armies. One of the most significant transformations in this regard is the emergence of hybrid aggression, a type of conflict that simultaneously integrates traditional combat methods with information warfare, cyberattacks, economic pressure, and even public opinion manipulation (Grigore 2015).

This major shift in the dynamics of conflict poses new challenges for the decision-making processes of states and international organisations involved in crisis management. In the face of a hybrid threat, decisions must be made in a context characterised by uncertainty, speed, and complexity. Thus, decision-making pragmatism becomes a key factor, especially in crisis situations, where every choice has the potential to influence the course of the conflict.

In this era of hybrid warfare, decisions are no longer merely a matter of strategic options on the battlefield; they also encompass areas such as cybersecurity, critical infrastructure protection, international relations management, and the coordination of public information and mobilisation efforts. Therefore, authorities must adopt innovative and flexible approaches that allow for quick and adaptable responses in the face of an unpredictable and multifaceted enemy.

In this context, the decision-making process becomes essential not only for military strategy but also for safeguarding the social and economic integrity of the state. Hybrid aggression presents political leaders, government institutions, and the military with complex dilemmas regarding available resources, coordination of actions, and prioritisation of objectives.

Thus, analysing decision-making pragmatism in the face of hybrid aggression addresses multiple fundamental dimensions of modern conflict. The response to this challenge is not limited to technical or military solutions, but requires the integration of a wide range of resources, from economic and political strategies to information management and the involvement of civil society. In this sense, decision-making pragmatism is not just a matter of efficiency, but an absolute necessity for ensuring the security and stability of a state in the face of a complex and often unforeseen attack.

## Hybrid Aggression – A New Paradigm of Conflict

Hybrid aggression represents a sophisticated and complex form of warfare, characterised by a synergistic combination of conventional and unconventional means, state and non-state actors, and both overt operations and covert tactics

(Ștefănescu 2024). The military component of hybrid aggression is subtle but highly effective, as it involves the use of armed forces in an indirect and strategic manner, often under the guise of civilian or non-military actions.

One of the most striking features of hybrid aggression is the use of military force below the threshold of conventional war, thereby avoiding a direct international response. For example, in the case of the annexation of Crimea, Russian armed forces operated without official insignia, leading to their being labelled as "little green men." This technique allowed Russia to maintain a degree of plausible deniability and avoid an open military confrontation with NATO.

Moreover, the military means employed in a hybrid conflict are often accompanied by intense disinformation campaigns, psychological destabilisation, and information warfare, aimed at weakening the morale of the target state's armed forces and sowing confusion among the population. "Shock and awe" tactics no longer require massive bombings, but instead may involve cyberattacks on critical infrastructure, disrupting power grids, communications, and military logistics.

Special forces play a crucial role in hybrid aggression. These well-trained units can carry out reconnaissance, sabotage, infiltration, and influence operations among local populations. Their missions are generally fast, efficient, and difficult to directly attribute to a state actor. These forces are also logistically supported by a parallel civilian infrastructure, allowing them to operate covertly in seemingly peaceful environments.

Technology has a decisive impact on the military component of hybrid warfare. Drones, surveillance satellites, facial recognition technologies, and big data analytics software are used to gain strategic advantages without the need for massive troop deployment. As a result, instead of a traditional battlefield confrontation, we see an invisible but lethal battle fought simultaneously on multiple fronts.

Another important aspect of hybrid aggression with a military focus is the exploitation of local conflicts or ethnic tensions to legitimise so-called "humanitarian" interventions or actions to "protect minorities." Under this pretext, the aggressor's armed forces are deployed to foreign territories with the apparent goal of maintaining peace, but in reality, they contribute to territorial occupation and manipulation of local power structures.

In addition to all of this, the importance of modern military doctrines cannot be underestimated. States that are potential victims of hybrid aggression must adapt their military strategies, modernise their armed forces, and invest in the training of specialised units for rapid response, urban warfare, and cyber defence. Doctrinal flexibility and rapid response capability are essential to counter the effects of hybrid aggression.

Therefore, the military dimension of hybrid aggression does not manifest through classical invasions, but rather through a subtle, persistent, and multidimensional presence. To counter this type of threat, a profound reconfiguration of how military capabilities are conceived and employed is necessary, integrated with the broader framework of national security.

## The Foundations of Decision-Making Pragmatism in Crisis Situations

In the context of hybrid aggression, the decision-making process is subjected to unprecedented pressure, as political and military leaders must manage a type of conflict that does not follow traditional patterns. Within this framework, decision-making pragmatism is not merely an efficient option but an imperative necessity. Pragmatism means orienting decisions toward concrete results, efficiency, adaptability, and flexibility, while avoiding the pitfalls of ideological rigidity or decisions based solely on precedent.

In crisis situations characterised by uncertainty, time pressure, and an imbalanced flow of information, decision-makers must adopt an approach based on continuous analysis of risks and opportunities (Dumitru 2022). The fundamental elements of such pragmatism include:

**1. Real-Time Contextual Evaluation** – Decision-making pragmatism requires constant adaptation to the dynamics of the threat. In the case of hybrid aggression, the unpredictable nature of events demands continuous monitoring of the operational environment using multiple sources: military intelligence, diplomatic channels, media, and open-source analysis.

**2. Strategic Flexibility** – A core principle is the avoidance of rigid planning. Under hybrid aggression, where the adversary's tactics shift rapidly, response strategies must be modular, scalable, and reversible. This implies having predefined scenarios, as well as the ability to adjust them in real time.

**3. Data-Driven Decision Making** – Instead of impulsive reactions or intuition-based decisions, pragmatism promotes the use of data-driven analysis: predictive models, simulations, and machine learning algorithms. These tools support rational decision-making—concise, informed, and grounded in reality.

**4. Rapid and Accountable Decisions** – In the context of a hybrid attack, delaying decisions can lead to devastating consequences. Pragmatism involves accelerated decision-making processes and an institutional culture where accountability is encouraged. Effective leaders must act under uncertainty and be ready to correct course as the situation evolves.

**5. Interinstitutional and Multidisciplinary Collaboration** – Decisions can no longer be made in isolation. In the face of hybrid aggression, where military, economic, cyber, and social dimensions are simultaneously targeted, collaboration among institutions is essential: military, intelligence services,

government, academia, and the private sector.

**6. Adaptive Thinking and Anticipatory Leadership** – A pragmatic leader anticipates crisis scenarios and prepares the organisation for response and resilience. This means fostering a learning culture in which lessons from past crises are documented and translated into viable policies.

Beyond these operational and strategic elements, decision-making pragmatism is also influenced by the individual traits of decision-makers: emotional intelligence, stress management ability, empathy, and communication skills. In an environment marked by informational chaos and social panic, a leader's ability to project calm and coherence becomes a crucial vector of stability.

The foundations of decision-making pragmatism in crisis situations are deeply rooted in the complex realities of the 21st century, where hybrid aggression demands a profound reconfiguration of decision-making mechanisms. This modern paradigm cannot be reduced to simple manuals or doctrines, it must become an integral part of organisational culture, leadership education, and institutional architecture. Only through such a coherent and multidimensional effort can an effective, legitimate, and sustainable response to contemporary hybrid threats be ensured.

## Decision-Making Tools and the Management of Hybrid Aggression

Managing hybrid aggression involves a complex set of decision-making tools capable of responding to the multifaceted challenges of modern conflict. These tools must integrate strategic, operational, and tactical dimensions within a coordinated and adaptive action framework (Dojan 2016). In this context, the role of the pragmatic decision-maker is to select and operationalise the most appropriate tools, depending on the nature of the aggression, the scope of the threat, and the internal capabilities available (Cullen 2017).

**1. Integrated Early Warning Systems (IEWS)** – These represent the first line of defence against hybrid aggression (Botea 2019). The early collection and analysis of weak crisis signals from multiple sources – social, economic, military, and cyber – enable the activation of response mechanisms before the effects become critical. Pragmatic decision-making involves the efficient real-time use of these tools, avoiding decision paralysis.

**2. Interagency Crisis Cells** – In the face of hybrid threats, an effective response requires a multisectoral approach. Creating crisis cells with representatives from defence, public order, intelligence, strategic communication, and the private sector ensures a collective decision-making process, based on the rapid sharing of information and the ability to act simultaneously on multiple fronts.

**3. Simulations and Wargaming** – These tools allow for the testing of hybrid aggression scenarios in a controlled environment. They help

identify vulnerabilities, test decisions under stress conditions, and refine institutional responses. Pragmatic decision-makers use these exercises not only for preparedness but also to develop an organisational culture focused on anticipation and adaptation.

**4. Artificial Intelligence-Assisted Decision Platforms** – In the digital age, AI can process vast amounts of data to provide rapid and precise decision support. Machine learning algorithms can detect behaviour patterns, anticipate hybrid actors' moves, and suggest response options. The implementation of these platforms must be done cautiously, ensuring constant human oversight over critical decisions.

**5. Strategic Communication and Counter-Narratives** – Hybrid aggression often includes a strong informational component. Combating disinformation and manipulation requires clear mechanisms of strategic communication through which the state can convey coherent, credible, and synchronised messages. Pragmatic decision-makers must understand the importance of this dimension and integrate it into the response architecture.

**6. Societal Resilience Mechanisms** – An effective response to hybrid aggression cannot exclude the civilian population. Pragmatic decision-making also involves investment in civic education, digital literacy, volunteerism, and community infrastructure – all aimed at reducing vulnerability to manipulation and supporting social cohesion (Buica 2022).

**7. Legal and Normative Instruments** – Responding to hybrid aggression requires a legal framework that enables rapid interventions without sacrificing democratic values. Pragmatic decisions must be legally sustainable, and the normative framework must be periodically revised to keep pace with the evolving nature of threats.

The decision-making tools used to manage hybrid aggression must reflect a holistic and integrative approach, so that they are aligned with each other through a clear, coordinated, and pragmatic decision-making process. Effective leaders are those who understand the complexity of these tools, select them based on context, and apply them in a flexible yet firm manner. Only in this way can a coherent and effective response be ensured in an increasingly fluid and challenging geopolitical landscape.

## Decision-Making Pragmatism in the Context of the Conflict in Ukraine

The conflict in Ukraine, which began in 2014 and escalated in 2022 with the full-scale invasion by the Russian Federation, represents a relevant example of the application of decision-making pragmatism in a hybrid aggression context. The war in Ukraine combines conventional warfare techniques with cyber operations, information warfare, economic pressure, and manipulation of public opinion. Faced with this complex hybrid threat, Ukrainian authorities were forced to make rapid and effective decisions to protect national territory and maintain internal

stability, demonstrating their ability to respond flexibly and adaptively in a fluid and unpredictable environment (Lesenciuc 2023).

**The Context of Hybrid Aggression in Ukraine**

The 2022 Russian invasion intensified hybrid aggression, as the Russian Federation combined conventional tactics with cyberattacks, disinformation campaigns, public opinion manipulation, economic pressures, and attempts to destabilise society (Stancu 2019). Russia employed multiple hybrid tools to destabilise Ukraine and gain a strategic advantage, and Ukraine's response was marked by pragmatic decision-making. The hybrid methods used by Russia and Ukraine's responses are analysed in greater detail in the following sections.

**Hybrid Tools Used by the Russian Federation**

The Russian Federation employed a complex combination of hybrid tools to destabilise Ukraine and undermine its government (Giurgea 2024):

- **Cyberattacks:** Before and after the 2022 invasion, Russia launched a series of cyberattacks against Ukraine's critical infrastructure, including power systems, communication networks, and banking systems. These attacks aimed to paralyse state institutions and create panic among the population.
- **Information warfare and disinformation:** Another hybrid method was the massive disinformation campaign. Kremlin spokespersons and state-affiliated media launched propaganda efforts to manipulate public opinion in Ukraine and internationally by spreading fake news, conspiracy theories, and messages that undermined trust in Ukrainian authorities.
- **Economic pressure:** Russia imposed economic sanctions and trade blockades to undermine Ukraine's economy. It also blocked Ukrainian ports and disrupted supply chains for vital resources.
- **Undermining internal political structures:** Russia used internal destabilisation tactics to create chaos among the Ukrainian population. These included attempts to stoke ethnic and sectarian conflicts and fuel internal discontent and divisions among different groups of Ukrainian citizens.

**Ukraine's Pragmatic Response to Russia's Hybrid Tactics**

Ukraine's response to Russia's hybrid aggression was characterised by decision-making pragmatism. Ukrainian authorities quickly adopted adaptable and effective measures to counter each of the hybrid tools employed by Russia:

- ✓ **Cyber defence response:** In the face of cyberattacks, Ukraine collaborated closely with international partners, including NATO and cybersecurity companies, to strengthen its national cyber infrastructure. Swift measures were implemented to restore affected systems and protect critical infrastructure, demonstrating rapid and flexible decision-making in safeguarding national security.
- ✓ **Disinformation counter-campaigns:** Ukraine implemented information warfare strategies, using social media and mass media to provide accurate

information to the population and combat Russian propaganda. Efforts included identifying and eliminating sources of disinformation and working with international social media platforms to limit the spread of fake news. The Ukrainian president played a central role in these campaigns with an active social media presence and direct communication with Ukrainian citizens and the international community.

- ✓ **International support and strategic alliances:** Ukraine swiftly sought assistance from international partners, such as NATO, the European Union, and the United States. This support included not only weaponry but also financial aid and economic assistance to help stabilise Ukraine's economy under Russian pressure. Ukraine's pragmatic diplomacy secured a unified international response, isolated Russia, and bolstered global support for Ukraine.
- ✓ **Mobilisation of internal and external resources:** Ukraine quickly mobilised internal resources, including the military, territorial forces, and civilian volunteers, to defend the national territory. Simultaneously, authorities engaged civilians in various activities, such as defence equipment production and logistics, thereby strengthening national resilience. The rapid mobilisation of reservists and the integration of local communities into defence efforts were clear examples of effective decision-making pragmatism.
- ✓ **Protection of vital infrastructure and economic adaptation:** Ukraine implemented quick measures to protect its energy and economic infrastructure, reorganising resource distribution and finding alternative energy supply solutions. Authorities also adopted flexible economic policies to maintain financial stability despite Russian-imposed economic sanctions.
- ✓ **Rapid development of the "Diia" application:** This digital tool was essential in crisis management, providing a constant flow of information and assistance to Ukrainian citizens. The app facilitated efficient government communication and resource coordination, allowing citizens quick access to official documents, real-time crisis alerts, and participation in mobilisation processes.
- ✓ **Online recruitment campaigns:** Ukrainian authorities quickly launched online platforms to encourage citizens, including those in the diaspora, to join national defence efforts. These platforms demonstrated the authorities' rapid adaptation to the immediate needs of the conflict.
- ✓ **Use of civilian safety and location apps:** Authorities launched applications and platforms that enabled the safe location of civilians, coordination of evacuations, and information about safe shelters.

These measures illustrated Ukraine's decision-making pragmatism, enabling a swift and adaptive response to each phase of the hybrid aggression. These actions were essential for maintaining internal cohesion and ensuring that both internal and external resources were used effectively.

Ukraine's pragmatic decision-making was also reflected in the resilience and adaptability of Ukrainian society in the face of hybrid aggression. The population showed remarkable resilience to Russian attacks and internal pressures, actively participating in national defence efforts. Public information campaigns, citizen education, and support for civilians actively involved in protecting their territories were essential for maintaining morale and social cohesion. Civic spirit and active public engagement across various areas of national defence were key factors contributing to Ukraine's initial success in countering Russia's hybrid aggression.

The decision-making pragmatism of Ukrainian authorities, combined with international support and active public involvement, was fundamental in countering Russian hybrid aggression and maintaining a coherent and effective long-term response. This case study highlights the importance of decision-making flexibility and adaptability in an extremely volatile security environment, such as that of hybrid aggression.

## Conclusions

In today's era, marked by geopolitical instability, the proliferation of emerging technologies, and the volatility of non-state actors, hybrid aggression represents a complex, adaptive, and persistent threat. In this landscape, decision-making can no longer be an isolated, bureaucratic, or linear process, but must transform into a continuous exercise of pragmatism and anticipation. Thus, decision-making pragmatism becomes a criterion for strategic survival in the face of hybrid aggression, and in an environment dominated by ambiguity and ambivalence, the decision-maker's ability to act quickly, flexibly, and based on continuous risk assessment is crucial. Pragmatism in this context means abandoning dogmatism and continuously adapting to the changing realities of the operational environment, with decision-making becoming an act of balancing what is possible, feasible, and acceptable at a given moment.

Institutional interoperability, artificial intelligence, big data analysis, and strategic simulations are the central pillars of modern decision-making infrastructure. In a hybrid conflict where reaction time is critical, the ability to integrate multiple sources of information and extract relevant patterns in real time from large data volumes can make the difference between success and failure. Moreover, interoperability between civilian and military structures, as well as between national and international bodies, is fundamental to avoiding dysfunctions and overlaps that adversary parties could exploit.

Another critical element in the hybrid conflict landscape is adaptive, reflective, and proactive leadership. Leaders must be not only skilled strategists but also empathetic, open to feedback, and capable of managing tensions between competing priorities.

They must make decisions under intense stress, mobilise their teams, and maintain organisational cohesion amid uncertainty. Their training should include not only military preparation but also the development of emotional intelligence, critical thinking, and strategic communication skills.
The societal dimension of the response involves an integrated vision of national security. Well-informed citizens, educated in resilience and aware of the mechanisms of hybrid aggression, become active partners in the defence of the country. Combating informational manipulation, promoting critical thinking, and strengthening trust in democratic institutions are essential actions to limit the tactical success of hybrid actors. Additionally, government communication must be transparent, coherent, and adapted to modern channels to build public trust.

Last but not least, normative frameworks and democratic mechanisms must be modernised to provide both operational flexibility and guarantees for the protection of citizens' rights. Decision-making pragmatism requires a delicate balance between reaction speed and adherence to the rule of law. Legislative reforms should include clearly defined emergency scenarios, rapid activation procedures for defence mechanisms, and public-private collaboration protocols, especially in critical areas such as cyber infrastructure, media, and the financial sector.

In conclusion, success in countering hybrid aggression does not depend solely on resources or technology but on the quality of the decision-making process. A pragmatic, informed, and strategically well-articulated approach can turn vulnerability into a competitive advantage and crisis into a catalyst for reform. In a world where the boundaries of conflict become increasingly blurred, it remains essential that the decision-making process be grounded in reality but oriented toward the future.

## References

**Botea, M.** 2019. „Despre războiul hibrid și contracararea efectelor acestuia." *Gândirea Militară Românească* nr. 2. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/GMR-2_2019.pdf.

**Buica, D.** 2022. *Dezinformarea, componentă a războiului hybrid.* București: Editura Universității Naționale de Apărare „Carol I".

**Cullen, P.** 2017. *Understanding Hybrid Warfare.* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf.

**Dojan, M.** 2016. *Rusia și războiul hibrid. Cazul Ucraina.* București: Editura Universității Naționale de Apărare „Carol I".

**Dumitru, I.R.** 2022. „Evoluția conceptului de război hibrid în strategiile naționale de apărare ale României." *Buletinul Universității Naționale de Apărare „Carol I"* 11 (3): 24-34. https://revista.unap.ro/index.php/revista/article/view/1484/1435.

**Giurgea, N.** 2024. *Războiul hibrid: Tehnici și strategii.* https://www.geopolitic.ro/2024/11/razboiul-hibrid-tehnici-si-strategii/.

**Grigore, L.** 2015. „Viitorul războiului – Războiul hibrid." *Buletinul Universității Naționale de Apărare „Carol I"* 2 (2): 187-191. https://revista.unap.ro/index.php/revista/article/view/135.

**Lesenciuc, A.** 2023. „Războiul hibrid în vreme de război - încercare de operaționalizare conceptuală și acțională." *Gândirea Militară Românească* nr. 1: 64-85. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2023%20gmr/gmr%201/LESENCIUC.pdf.

**Stancu, M.C.** 2019. „Războiul hibrid și forme de manifestare ale acestuia în criza din Ucraina." *Gândirea Militară Românească* nr. 2: 12-43. https://gmr.mapn.ro/webroot/fileslib/upload/files/arhiva%20GMR/2019%20gmr/2019/2%202019%20gmr/stancu.pdf.

**Ştefănescu, M.** 2024. *Războiul hibrid: O abordare complexă a confruntărilor moderne.* https://www.ziarultricolorul.ro/razboiul-hibrid-o-abordare-complexa-a-confruntarilor-moderne/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security

**Assoc. Prof. Florentina-Loredana DRAGOMIR, PhD***

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

## Abstract

With the intensification of hybrid threats, strategic organizations are faced with a fundamental challenge: ensuring a sustainable balance between process transparency, information confidentiality, and decision-making responsibility. This article analyzes the ethical triad of confidentiality, loyalty, and responsibility in the management of information systems in the field of national security, highlighting the need for information governance adapted to the current complexity. At the heart of the analysis is the role of intelligent information systems (IIS), which, by integrating artificial intelligence, machine learning, and behavioral analysis technologies, provide decisive support in modernizing security architectures and strengthening an ethical organizational culture. Intelligent information systems not only optimize threat detection and response processes but also actively contribute to the professionalization of strategic decisions by generating predictive assessments, automatic traceability, and alignment with legal regulations and ethical standards. They allow the transition from a reactive security model to a proactive one, oriented towards anticipation, compliance, and distributed responsibility. In this sense, the article argues that the integration of IIS is no longer an optional technological choice, but a strategic necessity for organizations that manage classified information and critical resources. Through its multidisciplinary approach and theoretically and normatively grounded arguments, the study contributes to the delimitation of a robust conceptual framework regarding the ethical governance of information in national security institutions.

**Keywords:**
Intelligent Information Systems; National Security; Ethical Governance; Strategic Decision-Making; Confidentiality.

**Article info**
Received: 30 April 2025; Revised: 28 May 2025; Accepted: 30 May 2025; Available online: 27 June 2025

Citation: Dragomir, F.L. 2025. "Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security". *Bulletin of "Carol I" National Defence University*, 14(2): 296-310. https://doi.org/10.53477/2284-9378-25-31

The ethical management of information systems in the field of national security has become a major strategic challenge. Military and security institutions are faced with the need to balance the transparency of operational processes with the protection of sensitive information, in an environment where confidentiality, loyalty, and accountability are essential pillars of institutional trust. Military and security institutions are faced with the need to balance the transparency of operational processes with the protection of sensitive information, in an environment where confidentiality, loyalty, and accountability are essential pillars of institutional trust. In the current strategic climate, deeply marked by accelerated digitalization and geopolitical volatility, the protection of sensitive information is a priority objective for organizations in the field of national security. In parallel, the demands regarding the transparency of processes and institutional accountability are becoming increasingly significant, including in the military sector. Thus, a fundamental ethical dilemma emerges: how can a sustainable balance be ensured between the need for operational transparency and the imperatives of confidentiality?

Confidentiality is no longer just a technical issue, but a fundamental ethical dimension in the architecture of strategic information systems. Recent studies highlight that the effectiveness of information security is influenced by institutional and cultural factors, and the integration of these aspects into security strategies is essential for protecting sensitive data (Metin, et al. 2024). Research emphasizes that the performance of information security systems depends significantly on the institutional context and cultural values, and the incorporation of these factors into security policies is crucial for ensuring the protection of sensitive data (Xu, et al. 2025). The loyalty of personnel with access to classified information is another critical element. Deviant behaviors, such as violating security policies, can have serious consequences for the integrity of information systems. Behavioral analyses highlight the importance of a strong organizational culture and ethical leadership to prevent these risks (Metin, et al. 2024). At the same time, the loyalty of personnel with access to classified information is asserted as an essential link in the security chain. Ethical misconduct and human factor risks remain among the main vulnerabilities of information systems. Preventing these risks requires cultivating a strong organizational culture, rooted in values such as institutional commitment and professional discipline. Accountability, both at the individual and institutional levels, is essential in the governance of information systems. The implementation of clear policies and effective audit mechanisms contributes to ensuring the integrity and availability of information, crucial aspects for the optimal functioning of strategic organizations (Almomani, et al. 2023). On the other hand, responsibility in information governance involves both formal control mechanisms (audit, traceability, regulations) and the conscious assumption of the consequences of decisions taken at all structural levels. The implementation of a framework of distributed responsibility contributes to strengthening institutional resilience and public trust (Almomani, et al. 2023).

In this context, the present article aims to explore the ethical triad formed by confidentiality, loyalty, and accountability, analyzing how these values can be integrated into the management of information systems in the field of national security. Through a multidisciplinary approach, we will examine the ethical challenges and solutions that can contribute to strengthening information security in strategic organizations.

## 1. Confidentiality in Strategic Information Systems Architecture

### *1.1 Defining the Concept of Confidentiality in the Context of National Security*

Confidentiality, along with integrity and availability, is one of the three essential dimensions of information security, known as the CIA triad. In an operational sense, confidentiality involves protecting data from unauthorized access, ensuring that only authorized individuals or entities can view, manipulate, or distribute sensitive information.

Within national security organizations, this component takes on critical importance. Protecting strategic, military, or diplomatic information from compromise is not just a technical requirement, but an institutional obligation that supports state sovereignty and the functioning of the defense system. Classified information, if disclosed or accessed in an unauthorized manner, can lead to operational vulnerabilities, damage to international relations, or even loss of life in theaters of operations.

One of the fundamental conceptual models for implementing confidentiality is the Bell–LaPadula model. It was designed for military environments, where classification levels are rigorous, and proposes two main rules: simple security property ("no read up") and property ("no write down"). These rules aim to prevent access to higher-level information by users with lower authorizations, respectively blocking the unauthorized transfer of information from higher to lower levels. The application of this model contributes to maintaining a rigorous security hierarchy, in which the information flow is strictly controlled and documented.

Thus, confidentiality in the architecture of strategic information systems must be understood not only as a technological protection measure but also as an ethical and institutional responsibility, anchored in the national and international regulatory framework on information security.

### *1.2. Technological and procedural tools for ensuring confidentiality*

Protecting sensitive information within strategic information systems involves implementing a set of technological and procedural measures designed to prevent unauthorized access, interception, or compromise of data. These measures are integrated into a comprehensive security architecture that operates both at the level of the IT infrastructure and within organizational structures.

Data encryption is one of the most effective technological means of protecting confidentiality. Advanced cryptographic algorithms, such as the Advanced

Encryption Standard (AES), ensure the confidentiality of information both in transit and at rest, preventing access to its content in the absence of a valid key (NIST, 2001). In military environments, where data circulates through distributed and often vulnerable networks, encryption is accompanied by robust authentication protocols and digital signatures, which help validate the identity of users and the integrity of messages.

Another fundamental pillar of privacy protection is access control policies. These are governed by mechanisms such as Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which ensure that access to information is granted according to the functional responsibilities and authorization level of each user. In strategic institutions, where the degree of classification of data is high, these mechanisms are complemented by Mandatory Access Control (MAC) policies, which impose rigid and hierarchical restrictions, in accordance with the legislation on classified information. In addition to technological components, procedural tools play an essential role in guaranteeing confidentiality. Systematic auditing of IT activities, real-time monitoring of data access, and analysis of user behavior contribute to the rapid identification of possible security breaches (Kent and Souppaya 2006). In parallel, continuous staff training, carried out through institutional awareness and training programs, aims to reduce the risks associated with human error, which remains one of the most frequent causes of compromising classified information.

Therefore, ensuring confidentiality is not limited to the implementation of high-performance technologies but requires integrated governance of information risk, in which processes, policies, and individual behaviors are in a relationship of strategic interdependence.

***1.3. Risks associated with the disclosure or loss of classified data***

Unauthorized disclosure or loss of classified information represents one of the most serious vulnerabilities in the architecture of strategic information systems, with direct implications for national security, geopolitical stability, and the operational capacity of military institutions. These incidents can compromise tactical plans, reveal technical capabilities, or affect strategic alliances and partnerships, generating a domino effect in decision-making and operational chains.

First of all, compromising classified information can lead to the loss of strategic advantage. In an operational environment where information asymmetry is decisive, adversaries' access to sensitive data can favor actions of anticipation, deterrence, or sabotage, which undermine the efficiency and safety of military missions. Cases documented in the specialized literature reveal that information leaks within defense institutions have repeatedly led to the reassessment of command structures, the temporary suspension of operations, and the diminution of inter-institutional trust.
Second, the loss of control over classified data severely affects international relations

and security cooperation. Strategic partners base their information exchange on the premise of mutual confidentiality and the existence of equivalent information protection measures. A breach in this system of trust can lead to the restriction of access to critical information, the suspension of collaborations, or the reassessment of the geopolitical position of the affected state.

From an institutional perspective, such incidents generate significant costs, both logistically and in terms of reputation. Reconfiguring the affected systems, initiating internal investigations, remedial measures, and additional investments in security involve the allocation of considerable budgetary resources. Moreover, in the context of public opinion, the loss of sensitive information can erode citizens' trust in the state's ability to protect its fundamental interests, fueling the perception of institutional vulnerability. To mitigate these risks, strategic organizations must adopt a proactive approach, based on ongoing risk assessments, penetration testing, incident simulations, and independent audits. These mechanisms must be supported by a coherent regulatory framework and an organizational culture oriented towards compliance, accountability, and information vigilance. Without these measures, the protection of classified data remains exposed to persistent, sophisticated, and systemic threats.

With the growth of strategic data and the rise of hybrid threats, protecting sensitive information can no longer be effectively achieved through traditional security and institutional control mechanisms. This article has argued that the ethical triad of confidentiality, loyalty, and accountability cannot be sustainably supported without the integration of emerging technologies, especially intelligent information systems (IIS).

These systems not only extend the technical capabilities of strategic organizations but also fundamentally transform the way information governance is understood and applied. With the ability to monitor user behavior in real time, generate predictive risk assessments, and support strategic decisions through recommendations that comply with ethical and legal standards, IISs become distributed accountability infrastructures. They provide additional guarantees for the integrity of processes and significantly reduce the risk of human error, abuse, or institutional negligence.

Another essential contribution of these technologies is to support an ethical organizational culture. Through traceability, impartiality in evaluation, and adaptability, SII contributes to strengthening the professional awareness of staff and to the internalization of institutional values. Thus, technology functions not only as a control tool, but as a mechanism for cultivating institutional ethics, in which responsibility is not imposed externally, but supported by infrastructure and decision-making process.

The integration of intelligent information systems into the architecture of strategic organizations must be seen not as a technological option, but as a strategic

necessity. They provide the premises for robust, compliant, proactive, and value-oriented governance. In an increasingly unstable information environment, where reaction time is critical and the costs of mistakes are irreversible, SII constitutes an indispensable support for ensuring security, legitimacy, and institutional resilience.

## 2. Institutional and individual responsibility in the governance of information systems

### *2.1. Normative frameworks and legal obligations regarding information protection (national laws, international treaties)*

Responsibility in the field of information governance is closely correlated with compliance with a complex normative framework, which brings together national regulations, international directives, and multilateral treaties regarding the protection of classified data and critical infrastructures. In Romania, Law no. 182/2002 on the protection of classified information, together with the related methodological rules, establishes the obligations of public institutions and authorized personnel regarding the classification, handling, and storage of sensitive data. These provisions are harmonized with NATO and EU requirements regarding interoperability in the field of secured information.

At the international level, instruments such as the NATO Information Security Treaty and the General Data Protection Regulation (GDPR) – where the interaction also involves civilian or dual-use components – impose clear standards regarding confidentiality, traceability, and responsibility for information processing. Also, conventions such as the Budapest Convention on Cybercrime outline state obligations in preventing and combating illegal access to systems and data.

Compliance with these rules is not optional, but is part of the institutional responsibility to guarantee information security as an integral part of national security. This responsibility presupposes the existence of functional internal control structures, periodic auditing, and continuous updating of procedures in accordance with technological developments and emerging threats (Dragomir-Constantin 2025c).

### *2.2. Accountability mechanisms: traceability, auditing, criminal or disciplinary liability*

In the context of information systems used by strategic organizations, responsibility cannot be reduced to a theoretical principle or an abstract value; it must be expressed concretely through a set of institutionalized mechanisms that allow both the prevention and remediation of incidents that affect the confidentiality of classified information. This responsibility is twofold: individual, in the sense of the assumption of decisions by each authorized user, and institutional, through the existence of structures and procedures that ensure the traceability of actions, the auditing of

systems, and the application of sanctions in case of misconduct. Traceability is the fundamental condition for any form of accountability. By implementing technical monitoring mechanisms, such as activity logging, cryptographic journaling systems, and behavioral analysis platforms, organizations can ensure continuous visibility of user interactions with critical systems. Thus, each access, modification, or transmission of data is recorded and associated with a digital identity, eliminating the premises of anonymity and reducing the risk of impunity (Dignum 2019). This system of tracking individual actions is indispensable for identifying the source of an incident, but also for establishing proportional responsibility.

Audit, as a formal tool for verifying compliance and efficiency, contributes to maintaining a transparent and predictable institutional climate. Periodic assessments of information security policies, carried out by internal or external entities, allow not only to correct deviations, but also to anticipate structural vulnerabilities. In military environments, audit has an additional strategic dimension: it validates the capacity of information systems to support operations under conditions of informational and cyber adversity (Kent and Souppaya 2006).

Disciplinary and legal sanctions complete this framework, ensuring a proportionate institutional response to violations of security norms. Without clear sanctioning mechanisms, responsibility becomes illusory, and the organization runs the risk of the norms being perceived as purely formal. The consistent application of measures – from withdrawal of access, to temporary or permanent suspension from office, to criminal prosecution in serious cases – contributes to the consolidation of an institutional culture based on compliance with regulations and awareness of the individual consequences of negligence or malicious intent (Metin, et al. 2024).

Thus, accountability in a strategic information ecosystem cannot function in the absence of a coherent framework of traceability, audit, and sanctioning. This institutional triad ensures not only operational resilience but also the internal and external legitimacy of the organization in the face of the challenges specific to the contemporary security environment.

Traceability is an essential functionality within the security architecture of strategic information systems, defining the system's ability to record, track, and correlate all actions carried out on information resources by authorized users. This function is not only a technical role, but also constitutes the foundation of individual and institutional accountability, providing evidentiary support for assessing user behavior and process compliance with policies and regulations in force. Operationally, traceability is achieved through a set of technologies and methods, such as detailed access logs, cryptographic journaling systems, and behavioral analysis modules, which allow the correlation of each action in the system with a unique digital identity. In high-security military and institutional environments, these systems are configured to operate in a non-repudiation regime, ensuring that

no relevant operation can be subsequently contested by the actor that generated it (Sulaiman, et al. 2022).

The importance of traceability is not limited to the post-incident investigative dimension, although this is vital for determining the causes and responsibilities in the event of information compromise. It plays a preventive and systemic role in the information risk governance process, allowing institutions to monitor user activity in real time, detect behavioral anomalies, and react promptly to violations or potential internal attacks. Thus, traceability contributes to strengthening operational response capacity and maintaining an organizational culture based on transparency and accountability. In addition, traceability is an essential condition for effective auditing of information systems. Especially in strategic organizations, logs must be protected against modification or deletion, as they can constitute legal evidence in disciplinary or criminal investigations. For this reason, military institutions implement solutions that ensure the integrity of logs through digital sealing mechanisms, temporal synchronization with external time sources, and replication in redundant systems, thus guaranteeing that any attempt to alter records is detectable and punishable.

Therefore, traceability is not only a technological component but a strategic dimension of the security architecture, integrated into the overall compliance, internal control, and information governance policies. Without a robust traceability mechanism, strategic institutions risk not only losing control over information resources but also diminishing the ability to react legitimately and effectively to internal misconduct or external attacks.

Auditing is one of the most important components of the institutional control mechanism in information security, with the role of assessing the compliance, efficiency, and robustness of processes, policies, and IT infrastructures. In strategic environments, auditing transcends the purely procedural dimension, becoming an essential tool for governance and risk anticipation, which contributes to strengthening organizational integrity and maintaining operational capacity in conditions of uncertainty or threat. Information security auditing is carried out on two interdependent levels: the technical and the procedural. The technical audit involves examining information systems from the perspective of security configurations, encryption levels, intrusion detection systems, as well as access and logging policies. The objective is to identify vulnerabilities that could be exploited by internal or external actors and assess the system's ability to withstand cyberattacks, including advanced persistent threats (APT). In military organizations, this type of audit is often complemented by penetration simulations ("red teaming"), in which specialized teams attempt to compromise systems in a controlled manner to highlight weaknesses in the defense.

On the other hand, procedural auditing focuses on how security policies and regulations are applied in practice. It analyzes the compatibility between operational

flows and regulatory requirements, the degree of compliance with protocols for accessing and handling classified information, and the level of training of personnel. Discrepancies between theoretical provisions and the actual behavior of institutional actors may signal communication deficiencies, the lack of an organizational culture focused on security, or even systemic risks generated by tolerance for deviations. An effective audit requires the independence of control structures, access to unfiltered data, and the ability to formulate operational recommendations, not just technical findings. It is also essential that the audit results are integrated into a continuous improvement cycle, in which recommendations are translated into concrete measures and their implementation is monitored with the same rigor.

In conclusion, auditing is not just a retrospective verification practice, but an active element of the information security system, designed to detect and correct vulnerabilities, validate measures, and strengthen individual and institutional responsibility. In the absence of a solid audit function anchored in the decision-making architecture of strategic organizations, control over information risks remains partial and reactive, which can compromise the resilience of the entire system.

Legal and disciplinary liability is the sanctioning dimension through which strategic organizations strengthen their control mechanisms and prevent non-compliant behaviors. In highly classified environments, such as military ones, individual responsibility for protecting classified information is not only a professional obligation but also a legal requirement, regulated by internal rules, national legislation, and international treaties on security and defense. Within military institutions, the sanctioning regime is complemented by internal regulations that include, in addition to temporary suspension or revocation of access to classified information, procedures for demotion or exclusion from the system. Criminal liability is activated when the compromise of information occurs through intentional acts, gross negligence, or culpable omissions. Such acts include the unauthorized transfer of data, unauthorized access to classified systems, loss of physical storage media, or failure to comply with operational procedures. In these cases, the competent authorities, including specialized structures of the Public Ministry or counterintelligence services, initiate investigations that may lead to the prosecution of the individuals involved (Metin, et al. 2024). Disciplinary liability, although distinct from criminal liability, plays a complementary role, with the objective of maintaining internal order and compliance with organizational norms. This can be applied even in situations where the act does not meet the constitutive elements of a crime, but reflects unacceptable conduct from the perspective of job obligations. Sanctions can range from written warnings and temporary salary reductions to dismissal from office or exclusion from security structures, depending on the seriousness of the violation and the position occupied by the person in question.

In strategic environments, the effectiveness of these forms of liability depends on three factors: the clarity of the rules, the consistency of application, and the

transparency of the procedures. The lack of a well-defined regulatory framework or the selective application of sanctions can lead to the erosion of the organizational culture based on ethics and responsibility. In contrast, a firm but fair liability regime contributes to strengthening internal trust, preventing information risks, and protecting the integrity of classified systems.

Thus, legal and disciplinary liability must be understood as an essential link in the information security ecosystem, through which individual behavior is correlated with institutional norms, and protecting sensitive information becomes an act of compliance, loyalty, and respect for the national interest.

## 3. Contributions of Intelligent Information Systems in Strengthening Organizational Responsibility and Ethics

In the era of accelerated digital transformation and intensification of hybrid threats, Intelligent Information Systems (IIS) have become essential elements in the architecture of strategic organizations, redefining the paradigms of governance, security, and decision-making. These systems, based on artificial intelligence (AI), machine learning (ML), predictive analytics, and cognitive automation processes, extend the functionalities of traditional information infrastructure, offering an increased capacity for adaptation and anticipation in volatile operational environments (Dignum 2019; Xu, et al. 2024).

In particular, IIS allows the modernization of decision-making processes by reducing uncertainty and increasing the speed of reaction to information threats. Machine learning algorithms can analyze massive volumes of data in real time, identifying relevant patterns, anomalies, and weak signals that could indicate a security breach or deviant behavior by an internal user. This early detection capability, combined with automated response mechanisms, directly contributes to strengthening information resilience and preventing incidents with systemic impact (Grigaliunas, et al. 2024). Furthermore, intelligent systems facilitate proactive governance of information risks by generating predictive models and decision-making recommendations based on probabilistic threat assessment. These tools not only support tactical security processes but also allow for the alignment of operational decisions with pre-established ethical and legal standards. Thus, SIIs become ethical support tools in environments where rapid decisions must be compatible with national and international regulations on data protection and fundamental rights (Dignum, 2019; Tounsi and Rais 2021).

A key element that differentiates intelligent information systems (IIS) from classic security infrastructures is their ability to facilitate proactive governance of information risks, based on anticipation, adaptation, and regulatory compliance. This proactive approach involves moving beyond the reactive paradigm, in which

security measures are implemented post-factum, and moving to a predictive model, in which threats are identified, assessed, and neutralized before they materialize. IIS integrates machine learning algorithms and artificial intelligence models that process large volumes of data from heterogeneous sources – including system logs, communication flows, behavioral profiles, and threat indicators – to generate probabilistic assessments of emerging risks. Through these capabilities, systems can detect weak signals and correlate seemingly isolated events, identifying patterns that indicate abnormal, potentially dangerous activities before they become manifest (Tounsi and Rais 2021). This type of predictive analysis gives decision-makers a significant time advantage, allowing them to adopt preventive, not just corrective, security measures.

In addition to the technical dimension, SII also contributes to supporting a coherent ethical and legal decision-making framework. In strategic organizations, where decisions often have to be made under pressure and uncertainty, intelligent tools provide objective analytical support, reducing the risk of arbitrary or non-compliant decisions. For example, by integrating ethical rules or data protection compliance criteria, systems can assess decision-making options not only from the point of view of operational efficiency, but also from the point of view of compliance with legal norms and principles of law (Dignum 2019).

This "automated ethical assistance" function becomes crucial in sensitive areas, such as national defense, cybersecurity, or the protection of critical infrastructures, where decisions can simultaneously involve technical, human, and political consequences. SII can recommend options that minimize collateral risks, protect personal data, or respect fundamental rights, even in operational contexts where such dimensions are easy to neglect. Thus, these systems not only optimize the response to threats but also institutionalize a framework of distributed ethical responsibility, in which normative principles are incorporated into the algorithmic logic of action. In this sense, the role of SII transcends the function of technological support, becoming an integral part of a responsible decision-making mechanism, capable of integrating security, legality, and ethical criteria in real time. In a complex and hyperconnected information ecosystem, in which the boundaries between the operational and the normative are increasingly fluid, this ability to support decisions compatible simultaneously with the imperative of efficiency and with moral and legal requirements represents a major strategic advantage.

Another essential benefit of SII consists of supporting an ethical organizational culture. By continuously and impartially monitoring user interactions with information systems, these technologies provide a framework of distributed responsibility, in which each actor is aware that their actions are subject to an objective regime of evaluation and traceability. In this sense, technology functions not only as a data guardian but also as a moral compliance mechanism, reducing the space for deviations or opportunistic behaviors (Xu, et al. 2024).

In conclusion, intelligent information systems contribute to the modernization of security architectures and the professionalization of strategic decisions, providing indispensable technological support for achieving a sustainable balance between operational efficiency, accountability, and institutional ethics. In an environment where reaction time is critical and human errors can have irreversible consequences, the integration of SII is no longer an option, but a strategic necessity for organizations that manage classified information and critical resources.

One of the most relevant benefits of intelligent information systems (SII) within strategic organizations lies in their ability to support and strengthen an ethical organizational culture, in which behavioral norms, institutional values, and individual responsibility are continuously promoted, verified, and reinforced through transparent and impartial technological mechanisms. Unlike traditional compliance models, which are predominantly based on hierarchical supervision and periodic audits, SII offers the possibility of constant, scalable, and neutral monitoring of interactions between users and critical information resources. By automatically collecting and analyzing data on user activity, including file access, configuration changes, communication through internal channels, or activity outside of work hours, these systems can build behavioral profiles that allow the detection of significant deviations from institutional norms. This form of monitoring does not aim at repressive control, but rather at cultivating an environment in which organizational actors become aware that each action is subject to a form of objective evaluation, unmediated by subjective perceptions or interests (Xu, et al. 2024).

In this configuration, technology becomes a catalyst for individual responsibility, contributing to the internalization of ethical norms by users. The awareness that professional activity is visible and traceable not only discourages opportunistic behaviors but also encourages the adoption of compliant practices, in which compliance with policies is no longer perceived as an external obligation but as a norm integrated into the individual's professional identity. This distributed responsibility, supported by impartial and automated systems, has the advantage of reducing the room for maneuver for destructive actions, while strengthening trust in institutional control mechanisms.

Furthermore, SII can contribute to the development of an organizational climate in which moral compliance is not just a result of fear of sanction, but of understanding and assimilation of institutional values. By analyzing collective and individual behaviors, systems can generate useful information about dominant patterns, the organization's ethical vulnerabilities, and the need for training or cultural adjustment interventions. This type of analytical feedback allows decision-makers to adopt proactive organizational ethics policies, based on data, and not just on assumptions or reactive incidents (Tounsi and Rais 2018).
Through advanced capabilities for predictive analysis, anomaly detection, reaction automation, and decision assistance, SII provides operational support that goes

beyond the technical sphere and penetrates the normative and organizational dimensions of security. Thus, decisions are no longer made solely based on intuition or individual experience, but are supported by data, correlated with scenarios, assessed according to risks, and filtered through ethical and legal constraints. This recalibration of the decision-making process allows not only to minimize human errors, but also to strengthen legitimacy and transparency within strategic institutions (Dignum 2019).

In the contemporary operational context, in which reaction time is compressed and the pressure on institutional leaders is constant, rapid but compliant decisions become an imperative. In this equation, SII offers a competitive advantage through its ability to provide information in real time, learn from previous incidents, and generate adaptive solutions in the face of dynamic threats (Tounsi and Rais 2018). Moreover, by promoting an organizational culture based on transparency, traceability, and distributed ethics, these systems support the development of an agile institution, capable of operating in volatile environments without compromising its fundamental values. In this sense, the role of SII is not limited to a security tool, but extends to the status of critical infrastructure for responsible decision-making, strategic governance, and organizational resilience.

Therefore, in institutional environments that manage classified information, critical infrastructures, or national strategic stakes, the implementation of intelligent information systems can no longer be considered a luxury or an optional choice. It represents an imperative necessity for strengthening security, optimizing decisions, and ensuring institutional conduct in line with international standards of ethics, legality, and performance.

## Conclusions

With the growth of strategic data and the rise of hybrid threats, protecting sensitive information can no longer be effectively achieved through traditional security and institutional control mechanisms. This article has argued that the ethical triad of confidentiality, loyalty, and accountability cannot be sustainably supported without the integration of emerging technologies, especially intelligent information systems (IIS).

These systems not only extend the technical capabilities of strategic organizations but also fundamentally transform the way information governance is understood and applied. With the ability to monitor user behavior in real time, generate predictive risk assessments, and support strategic decisions through recommendations that comply with ethical and legal standards, IISs become distributed accountability infrastructures. They provide additional guarantees for the integrity of processes and significantly reduce the risk of human error, abuse, or institutional negligence.

Another essential contribution of these technologies is to support an ethical organizational culture. Through traceability, impartiality in evaluation, and adaptability, SII contributes to strengthening the professional awareness of staff and the internalization of institutional values. Thus, technology functions not only as a control tool, but as a mechanism for cultivating institutional ethics, in which responsibility is not imposed externally, but supported by infrastructure and decision-making process.

The integration of intelligent information systems into the architecture of strategic organizations must be seen not as a technological option, but as a strategic necessity. They provide the premises for robust, compliant, proactive, and value-oriented governance. In an increasingly unstable information environment, where reaction time is critical and the costs of mistakes are irreversible, SII constitutes an indispensable support for ensuring security, legitimacy, and institutional resilience.

## References

**Almomani, Iman, Aala Alkhayer, and Walid El-Shafai**. 2023. "E2E-RDS: Efficient End-to-End Ransomware Detection System Based on Static-Based ML and Vision-Based DL Approaches" Sensors 23 (9): 4467. https://doi.org/10.3390/s23094467

**Bell, David Elliott, and Leonard LaPadula**. 1973. "Secure Computer Systems: Mathematical Foundations. Technical Report MTR-2547", Vol. I. Bedford, MA: The MITRE Corporation. https://websites.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

**Dignum, Virginia.** 2019. "Responsible Artificial Intelligence: How to Develop and Use AI in a Responsible Way". Springer. https://link.springer.com/book/10.1007/978-3-030-30371-6

**Dragomir, Florentina-Loredana, and Gelu Alexandrescu.** 2017a. "Applications of Artificial Intelligence in Decision-Making Process". Bulletin of Carol I National Defense University 4(2): 56–61. https://cssas.unap.ro/en/pdf_periodicals/si63.pdf

**___.** 2017b. "The Axiomatic Character of Decision". Bulletin of "Carol I" National Defense University 6 (1): 16–22. https://www.ceeol.com/search/article-detail?id=548274

**Dragomir, Florentina-Loredana., Gelu Alexandrescu, and Florin Postolache.** 2018" Tools for hierarchical security ". The 14 the International Scientific Conference "eLearning and Software for Education", Bucharest, Carol I" National Defence University, April 19 - 20, Advanced Distributed Learning Association, vol. 4, pp. 34–38.

**Dragomir-Constantin, Florentina-Loredana.** 2025a. "Information System for Macroprudential Policies. "Acta Universitatis Danubius. Œconomica 21 (1): 48–57. https://dj.univ-danubius.ro/index.php/AUDOE/article/view/3254

**___.** 2025b. "Thinking Patterns in Decision-Making in Information Systems". New Trends in Psychology 7 (1): 89–98. https://dj.univ-danubius.ro/index.php/NTP/article/view/3255

**___.** 2025c. "Thinking Traps: How High-Performance Information Systems Correct Cognitive Biases in Decision-Making". New Trends in Psychology 7 (1) 99–108. https://dj.univ-danubius.ro/index.php/NTP/article/view/3257.

**Grigaliūnas, Šarūnas, Michael Schmidt, Rita Brūzgienė, and Smyrli Panagiota.** 2024. "Holistic Information Security Management and Compliance Framework". Kaunas University of Technology. https://epubl.ktu.edu/object/elaba:209322117/

**Kent, Karen, and Murugiah Souppaya.** 2006. "Guide to Computer Security Log Management. NIST Special Publication 800-92. National Institute of Standards and Technology". https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-92.pdf

**Metin, Bilgin, Fatma Gözde Özhan, and Martin Wynn.** 2024. "Digitalisation and Cybersecurity: Towards an Operational Framework." Electronics 13 (21): 4226. https://www.mdpi.com/2079-9292/13/21/4226

**Sulaiman, Nur Shafinas, Mohd Azlan Fauzi, Wendy Wider, and Jasmine Rajadurai**. 2022. "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review." Social Sciences 11 (9): 386. https://www.mdpi.com/2076-0760/11/9/386

**Tache, Florentina-Loredana, Postolache Florin, Nachila Cătălin, and Ivan Maria Alexandra.** 2010." Consulting in Electronic Commerce." Acta Universitatis Danubius. Œconomica 6 (3): 162–169. https://journals.univ-danubius.ro/index.php/oeconomica/article/view/707

**Tounsi, Wassim, and Hassen Rais.** 2018. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attack". Computers & Security 72. https://www.sciencedirect.com/science/article/abs/pii/S0167404817301839?via%3Dihub

**Xu, Yao, Jixin Wei, Ting Mi, and Zhihua Chen.** 2024 "Data Security in Autonomous Driving: Multifaceted Challenges of Technology, Law, and Social Ethics." World Electric Vehicle Journal 16 (1): 6. https://doi.org/10.3390/wevj16010006

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Using Agile Project Methodologies in Military Action Planning

**Lt. Ionuț-Alexandru RADU***

*"Carol I" National Defense University, Bucharest, Romania
e-mail: radu.alexandru@unap.ro

## Abstract

To improve the responsiveness and adaptability of decision-makers in the ever-changing and unpredictable world of contemporary military operations, flexible and adaptable approaches to planning are essential. Originally created for software development, Agile approaches offer a new way to increase the effectiveness and efficiency of planning in the military context through the use of project management. This study examines the application of Agile concepts - such as collaboration, flexibility, and iteration - to the planning of military operations. This study highlights the advantages and challenges of applying these concepts in a military setting, emphasising how they can improve strategic adaptability and rapid response times. Focusing on their development, fundamental ideas and various project management applications, the study summarises the body of research on Agile approaches. The main focus of the paper is on the way in which Agile frameworks such as Scrum and Kanban can be adapted for use in military contexts, emphasising teamwork, customer satisfaction and continuous improvement. Key studies show that by encouraging greater cooperation and adaptability, Agile approaches dramatically improve project performance in dynamic contexts. However, obstacles such as reluctance to adapt, lack of qualified staff and problems in scaling Agile methods are also reported.

**Keywords:**
Agile Methodologies; Scrum; Kanban; Project; Military Operations; Planning.

**Article info**
Received: 22 April 2025; Revised: 5 May 2025; Accepted: 12 May 2025; Available online: 27 June 2025

Citation: Radu, I.A. 2025. "Using Agile Project Methodologies in Military Action Planning."
*Bulletin of "Carol I" National Defence University*, 14(2): 311-325. https://doi.org/10.53477/2284-9378-25-32

Military operations are conducted in environments characterised by volatility, uncertainty, complexity and ambiguity. Agile project methodologies, originally created for software development, offer promising approaches to enhance the effectiveness of military planning in these dynamic environments. This paper examines how Agile frameworks can be adapted to military contexts, providing empirical evidence of their benefits while recognising the challenges of their implementation. Research shows that military organisations adopting Agile methods have achieved significant improvements in responsiveness, collaboration, and operational efficiency. Medium-sized projects using Agile methods have delivered greater customer benefits than traditional approaches, with notable success in military IT deployments. While organisational resilience and security concerns pose challenges, strategic implementation approaches that balance military hierarchical structures with Agile principles hold great promise for improving military operational capabilities.

## 1. Historical background and evolution of military planning

### *1.1. Traditional military planning approaches*

Military planning has historically used linear, sequential processes that emphasise comprehensive, advanced planning and strict hierarchical execution. These traditional approaches, while providing structure and clarity of command, often fail to respond effectively to rapidly changing operational conditions. Military organisations around the world have recognised this limitation in contemporary operational environments where threats evolve rapidly and information flows continuously.

Traditional military planning typically follows a "waterfall" approach, with sequential phases that include intelligence gathering, mission analysis, course of action development, comparison, approval, and execution. This methodology emphasises thorough analysis and detailed planning before execution begins (Tudose 2021). While this approach provides a comprehensive analysis of factors and clear direction, it suffers from significant limitations in dynamic environments. Once launched, these plans are difficult to modify without substantial disruption, creating rigidity that can be exploited by more agile adversaries.

As military leaders face increasingly complex and unpredictable operational environments, the limitations of traditional planning approaches have become more apparent. The quest for greater flexibility within military organisations has become the "requirement of the moment" in the digital age, as they seek to flatten organisational structures to speed decision-making and improve responsiveness. This recognition has led to increased interest in alternative planning approaches that can better accommodate uncertainty and change.

### *1.2. The emergence of Agile methodologies*

Agile methodologies emerged in the software development industry in the 1990s, culminating in the "Agile Manifesto" in 2001. This manifesto established four core values: individuals and interactions are more important than processes and tools; functional software is more important than complete documentation; collaboration with customers is more important than contract negotiation; and responding to change is more important than sticking to a plan. These values represented a significant departure from traditional "waterfall" approaches to development, which followed a linear, sequential process similar to traditional military planning (Agile Manifesto 2001).

The Agile approach introduced several key innovations in project management, including iterative development, self-organising teams, continuous customer feedback, and adaptation to changing requirements. These principles were initially applied to software development, but have since been extended to diverse domains including product development, marketing and organisational management. Agile's success in managing complexity and uncertainty in commercial environments has sparked interest in its application in military contexts.

The evolution of the software industry from waterfall to Agile approaches reflects the challenges faced by military organisations. As Gen. Ellen M. Pawlikowski, former commander of Air Force Materiel Command, explained in 2017, Agile is about continuous iteration: "You plan it, you build it, you release it, you get feedback. And you do it constantly." This iterative approach offers a potential solution to the adaptability challenges facing military operations (U.S. Air Force 2019).

## 2. Theoretical framework for implementing agile approaches in the military environment

### *2.1. Fundamental principles of Agile project management*

Agile project management is based on several fundamental principles that differentiate it from traditional approaches. First, it emphasises iterative development, breaking projects into small, manageable cycles that produce incremental value. Second, it prioritises adaptability, encouraging change rather than resisting it. Third, it focuses on collaboration, promoting self-organising, cross-functional teams working closely together. Fourth, it focuses on the customer, ensuring continuous alignment with user needs. Finally, it encourages continuous improvement by regularly reflecting and adapting processes (Daraojimba, et al. 2024).

These principles manifest in various practices within Agile. Daily stand-up meetings improve communication and problem-solving. Sprint reviews (in Scrum) provide regular opportunities for stakeholder feedback. Retrospectives allow teams to learn from experience and improve processes. Visual workflow management (in Kanban)

increases transparency and identifies bottlenecks. Together, these practices create a framework to respond effectively to changing requirements while maintaining focus on delivering value (Orlov, et al. 2021).

The iterative nature of Agile project management is particularly valuable in uncertain environments. Rather than trying to predict all requirements and plan everything in advance, Agile approaches recognise uncertainty and establish mechanisms for periodic reassessment and adaptation. This iterative approach allows teams to learn and adapt as they progress, making it well-suited for complex and dynamic environments such as military operations.

### *2.2. Parallels between military strategy and Agile philosophy*

Surprisingly, many Agile principles find parallels in traditional military strategy and tactics. The ancient Chinese military strategist Sun Tzu emphasised adaptability, rapid response, and exploiting changing circumstances - concepts that align closely with Agile philosophy. Research has explored these connections, highlighting how military strategy concepts can be translated into Agile development principles. For example, Sun Tzu's emphasis on adaptability and adjusting strategies according to the situation aligns with Agile's emphasis on responding to change (Tudose 2021).

Military doctrine has long recognised the importance of adaptability in uncertain environments. The concepts of mission command and commander's intent provide subordinate units the freedom to adapt their approach while maintaining alignment with overall objectives. This balance between autonomy and alignment reflects Agile's emphasis on self-organising teams working toward common goals (Tudose 2021).

The link between military strategy and Agile becomes particularly evident when examining the military's approach to VUCA (Volatility, Uncertainty, Complexity, and Ambiguity) environments - a concept that has also been applied to business contexts. Both military doctrine and Agile methodologies recognise the limitations of prediction and detailed planning in such environments, emphasising instead adaptability, learning, and decentralised decision making (Supriyadi, et al. 2023).

### *2.3. Adaptability and responsiveness in military contexts*

The ability to adapt quickly to changing circumstances is crucial in military operations. Soldiers typically operate in uncertain, hostile and ambiguous environments where rapidly changing scenarios are the norm. Traditional planning approaches often have difficulty maintaining relevance in such dynamic environments, as plans can become obsolete before they can be fully executed.

Adopting Agile methodologies allows military leaders to exert control while adapting to changing conditions that might otherwise disrupt operations. By breaking down operations into smaller iterations, maintaining continuous feedback loops, and empowering teams to adjust tactics based on the realities on the ground,

Agile approaches can enhance the military's ability to respond effectively to emerging threats and opportunities.
This increased adaptability can provide strategic advantages in conflict situations. Military theorists have long recognised that the ability to execute the OODA (Observe, Orient, Decide, Act) loop faster than adversaries provides a significant advantage. Agile methodologies, with their emphasis on rapid feedback and adaptation, can accelerate this loop, enabling military forces to outperform adversaries in dynamic environments (Toroi and Stanciu 2023).

## 3. Agile frameworks and their military applications

### *3.1. Scrum framework in military operations*

Scrum, one of the most widely used Agile frameworks, provides a structured but flexible approach to project management that can be adapted to military contexts. The framework organises work into time-framed iterations, called sprints, typically lasting 1-4 weeks. Each sprint begins with planning, includes daily synchronisation meetings, and concludes with review and retrospective sessions. A product owner prioritises work based on value, while a Scrum master facilitates the process and removes impediments (Schwaber and Sutherland 2020).

In the military environment, Scrum can be adapted to support operational planning and execution. Sprint planning sessions can include mission analysis and course of action development. Daily meetings serve as synchronisation meetings for operational teams, ensuring alignment and surfacing challenges. Sprint reviews provide structured opportunities to assess progress and adjust plans as conditions change. Retrospectives support after-action review processes and lessons learned, reinforcing organisational learning.

The US Army has successfully used Scrum to manage logistics operations in Iraq and Afghanistan, demonstrating its applicability beyond software development. By organising logistical support into sprints and maintaining regular synchronisation, these operations achieved greater responsiveness to changing needs while maintaining coordination between units. This application shows how the Scrum structure can provide a sufficient framework to ensure coordination while allowing the flexibility needed in dynamic environments (Orlov, et al. 2021).

### *3.2. Kanban implementation for logistics and military support*

The Kanban method provides a visual approach to workflow management that can be particularly valuable for logistics and military support functions. The method visualises work items on a whiteboard with columns representing workflow steps, limits work in progress to prevent overload, and focuses on optimising flow through the system. This visualisation makes bottlenecks immediately visible, allowing teams to address problems before they affect operations (Kanban University 2021).

In military contexts, Kanban can efficiently manage operational tasks, logistics and support activities. The US Navy has used Kanban to manage the development of software systems, demonstrating its military applicability. By visualising the status of tasks and limiting work in progress, logistics teams can focus their resources on critical priorities instead of spreading their efforts too thinly across multiple tasks (Abercrombie, Fullbright and Long 2016).

Kanban's emphasis on limiting work in progress aligns with the military principle of concentrating force, suggesting a natural fit between the two approaches. By visualising workflows and identifying bottlenecks, military units can ensure that resources are directed to the most critical tasks, increasing overall operational efficiency.

### *3.3. Hybrid approaches: Scrumban, Kanplan and Military Design Thinking (MDT)*

Recognizing that there is no single framework that fits all contexts, hybrid approaches have emerged that combine elements of different Agile methodologies. Scrumban combines the Scrum framework with Kanban flow optimisation, while Kanplan adds Scrum backlog concepts to Kanban, allowing teams that don't work iteratively to benefit from backlog preparation.

Similarly, the military has developed hybrid approaches that combine Agile principles with traditional military planning. Military Design Thinking (MDT) adapts the principles of design thinking to military contexts, creating an innovative and flexible command and control (C2) method. This approach maintains the necessary military structures while incorporating iteration, user-centeredness, and adaptability from Agile and Design Thinking approaches (Alaidaros, Omar and Romli 2021).

These hybrid approaches provide valuable flexibility by combining structure with adaptability. They recognise the reality that military organisations cannot completely abandon hierarchical structures and formal processes, but they can improve them with Agile principles. This balanced approach may be the most practical way forward for military organisations that want to become more adaptive while maintaining the necessary command structures.

## 4. Empirical evidence and case studies

### *4.1. Transnational analysis of military IT projects*

Empirical studies of military IT projects provide valuable insights into the effectiveness of Agile methodologies in military contexts. A cross-country study of IT projects in NATO countries and agencies found that projects using Agile methods delivered more benefits to customers than those using traditional methods. Medium-sized projects performed better than small and large projects, and customer

involvement had a positive effect on project success. Clear specification of objectives also had a statistically significant positive effect on project outcomes.

This research challenges the common assumption that traditional approaches are more suitable for military projects. Empirical evidence suggests that Agile methods can deliver superior outcomes, particularly in terms of benefits and customer satisfaction. The finding that medium-sized projects performed best indicates that Agile methods can be most effective when applied at an appropriate scale, neither too small to justify the overhead nor too large to be managed effectively (Orlov, et al. 2021).

The study also highlighted the importance of customer involvement - a core Agile principle - in project success. Military IT projects that benefited from active end-user participation were more likely to deliver benefits that met real operational needs. This finding supports Agile's emphasis on collaboration between developers and users throughout the project lifecycle.

***4.2. Diggerworks: an Agile success story in the military***

One of the most compelling cases of a successful Agile implementation in a military context is Diggerworks, the Australian defence organisation responsible for the design, development, and integration of combat equipment and clothing for soldiers. Following its move to Agile, Diggerworks has achieved remarkable results: productivity has increased by 400-600%, project delivery times have dropped from months to weeks in many cases, and employee satisfaction has increased significantly (Cebon and Samson 2012).

The Diggerworks case is particularly notable because it involves physical hardware rather than software, demonstrating the applicability of Agile beyond IT. The organisation was established in 2011 after Australian Senate hearings identified critical problems in procurement and supply chain arrangements for military equipment. By adopting Agile approaches that emphasise innovation and responsiveness, Diggerworks has dramatically improved its ability to deliver better equipment faster.

This success has prompted other military groups to consider adopting Agile, including Army R&D groups, personnel management, and major procurement projects. Even the Royal Australian Navy and Air Force have expressed interest, suggesting a growing recognition of the potential benefits of Agile across all areas of the military.

***4.3. US Air Force Agile Transformation***

The U.S. Air Force has adopted Agile methodologies to address challenges in software development and acquisition. Following the lead of organisations such as the Defence Innovation Unit (DIU), the Air Force is implementing a more modern and less bureaucratic approach to development that aims to deliver capabilities to warfighters faster and at lower cost (U.S. Air Force 2019).

One notable example is the Air Force's Kessel Run software development initiative, which utilises Agile methods to rapidly develop and deploy software capabilities. By adopting Agile practices, Kessel Run has significantly reduced development times, enabling more responsive support to operational needs. This initiative represents a departure from the Air Force's traditional "waterfall approach" to software development, which typically followed a sequential process with lengthy documentation and review requirements (Budden, et al. 2021).

These Air Force initiatives demonstrate how even large, traditionally hierarchical military organisations can successfully adopt Agile approaches. By starting with specific projects and demonstrating success, these initiatives create momentum for broader organisational change while addressing immediate operational needs.

## 5. Agile benefits in military operations

### *5.1. Improve responsiveness to changing conditions*

One of the main benefits of Agile methodologies in military contexts is increased responsiveness to changing conditions. Traditional military planning processes can be time-consuming and difficult to adjust once set in motion. Agile approaches, which emphasise iteration and adaptation, allow military units to react more quickly to changing circumstances while maintaining operational effectiveness despite uncertainty.

Research on military projects using Agile methods has shown significant improvements in cycle time and responsiveness. For example, the ISPAN program shortened cycle time by 45 months, demonstrating the time-saving potential of Agile approaches (Kniberg and Skarin 2010). Similarly, the Diggerworks experience has shown dramatic reductions in project delivery times from months to weeks (Cebon and Samson 2012). These improvements in responsiveness translate directly into operational advantages. In combat situations, the ability to adapt quickly to changing circumstances can determine success or failure. By adopting Agile principles, military organisations can enhance their ability to respond effectively to dynamic operational environments while maintaining the initiative and seizing opportunities as they arise.

### *5.2. Improving collaboration and information exchange*

Agile methodologies emphasise collaboration and communication within and between teams. In military contexts, this can lead to more effective coordination and information sharing, addressing the "stovepipe" problem often seen in military organisations where information remains siloed in separate units or systems (Tudose 2021).

Studies of military IT projects have found that customer engagement, a key aspect of Agile approaches, has had a positive effect on project success. By encouraging closer collaboration between developers and users, Agile methods ensure that solutions

meet real operational needs rather than assumed requirements. Beyond IT projects, Agile principles can improve collaboration in operational planning and execution. Practices such as daily meetings and regular reviews improve synchronisation between units and ensure that all stakeholders have a common understanding of the situation and plan. This improved collaboration can reduce friction, increase coordination, and ultimately improve operational effectiveness (Alaidaros, Omar and Romli 2021)..

***5.3. Increase operational efficiency and effectiveness***

Agile methodologies can improve the efficiency and effectiveness of military operations by focusing resources on prioritised tasks, reducing waste, and promoting continuous improvement through regular feedback and adaptation. Kanban's emphasis on visualising work and limiting work in progress helps military units identify bottlenecks and ensure that resources are allocated to essential tasks. Diggerworks' experience with a 400-600% increase in productivity demonstrates the potential efficiency gains of Agile approaches. By focusing on delivering incremental value, limiting work in progress, and continuously improving processes based on feedback, military organisations can potentially accomplish more with limited resources, addressing the perennial challenge of balancing strategies with available resources (Agile Manifesto 2001).

These efficiency improvements are particularly valuable in resource-constrained environments. By eliminating waste, focusing on high-value activities, and continuously improving processes, Agile approaches enable military organisations to maximise the impact of available resources. This efficiency can create strategic advantages by enabling faster capability development and deployment.

***5.4. Strategic adaptability and learning***

At the strategic level, Agile methodologies provide military organisations with increased adaptability and learning capabilities. The iterative nature of Agile approaches creates regular opportunities to assess progress, gather feedback and adjust course as necessary. This enables faster learning and adaptation than traditional approaches that rely on extensive post-operational analysis. Military strategy research suggests that adaptability and learning are critical factors in long-term success. By adopting Agile principles, military organisations can improve these capabilities, gaining strategic advantages over less adaptive adversaries. The ability to learn and adapt faster than adversaries creates opportunities to seize and maintain the initiative in dynamic environments. This strategic adaptability also supports innovation in the development of military capabilities. By creating shorter feedback loops between users and developers, Agile approaches enable faster identification and implementation of innovative solutions to operational challenges. This accelerated innovation cycle can provide significant advantages in capability development and deployment (Abercrombie, Fullbright and Long 2016).

.

# 6. Implementation challenges and considerations

### *6.1. Organisational and cultural barriers*

Despite its potential benefits, implementing Agile methodologies in military contexts faces significant organisational and cultural barriers. Military organisations have deep-rooted traditions and established ways of working that can be difficult to change. The hierarchical nature of military structures may seem to conflict with Agile's emphasis on self-organising teams and distributed decision making. For example, in international contexts, cultural differences may accentuate incompatibilities between self-organising Agile teams and rigid hierarchical structures (Šmite, Gonzalez-Huerta and Moe 2018).

Research on Agile adoption in government and military contexts has identified resistance to change as a common barrier. Cultural factors, including risk aversion and a preference for established processes, can impede the adoption of new approaches. Overcoming this resistance requires strong leadership support, clear communication of the benefits, and careful phased implementation that respects the necessary military command structures.

The military's traditional emphasis on extensive planning and formal documentation may also conflict with Agile's preference for functional solutions over comprehensive documentation. Finding an appropriate balance that maintains necessary documentation while eliminating unnecessary bureaucracy is a significant challenge for military Agile implementations (Alaidaros, Omar and Romli 2021).

### *6.2. Security and privacy concerns*

Military operations involve sensitive information and strict security requirements that can potentially conflict with Agile's emphasis on transparency and information sharing. Balancing security needs with collaborative practices is a significant challenge for military Agile implementations.

Classified information and compartmentalised access create practical barriers to the free flow of information that supports Agile collaboration. Teams may be unable to share certain information across organisational boundaries, limiting the effectiveness of collaborative practices. For example, the DIACAP process used for security assessment in DoD projects introduces significant delays that run counter to the fast pace of Agile methodologies (Chung and Nixon 2013).

Military organisations must develop adapted approaches that maintain the necessary security controls while preserving the core benefits of Agile. In addition, military systems often operate on isolated networks with restricted access, which complicates the implementation of digital collaboration tools that support Agile practices. Creative solutions that maintain security while enabling necessary collaboration as well are essential for successful military Agile deployments (Kniberg and Skarin 2010).

***6.3. Agile scaling for large-scale military operations***

Scaling Agile methodologies to large and complex military operations presents significant challenges. While Agile approaches work well for small, co-located teams, they become more difficult to implement in large, distributed organisations with multiple interdependencies - exactly the environment in which military operations typically take place. Research on scaling Agile in large organisations has identified coordination difficulties, alignment issues, and communication barriers as common problems. Military operations, which can involve thousands of people in multiple locations, face similar challenges in extending Agile approaches beyond small units or specific projects.

Several frameworks for scaling Agile have emerged in commercial contexts, including SAFe (Scaled Agile Framework), LeSS (Large-Scale Scrum), and Nexus.
For example, Saab has demonstrated the success of scaling Agile by coordinating over 100 Agile teams to develop the Gripen aeroplane, using daily stand-ups and synchronised sprints. Such examples emphasise the importance of adapting the Agile framework to the complexity of military projects while maintaining alignment between teams and strategic goals (Rigby, Sutherland and Noble 2018).

While these frameworks offer potential solutions, they need to be tailored to military contexts to account for specific hierarchical command structures and operational requirements. Developing military-specific approaches for Agile scaling is an important area for future research and innovation.

***6.4. Implementation strategies for military contexts***

The successful implementation of Agile methodologies in military contexts requires thoughtful strategies that recognise organisational realities while pursuing meaningful change. Research on organisational change suggests that incremental approaches are often more successful than radical transformations, particularly in established organisations with strong cultures.

An effective approach is to start with pilot projects in selected areas where Agile is most likely to succeed. These might include IT projects, logistics management, or training programs where the benefits of adaptability and rapid feedback are most evident. Successful pilots serve as examples and learning opportunities for wider implementation, creating momentum for organisational change (Daraojimba, et al. 2024).
For example, initiatives such as the U.S. Air Force's Kessel Run have utilised Agile methodologies for critical application development, achieving significant resource savings and improved operational planning (Budden, et al. 2021).
Hybrid approaches that combine elements of traditional and Agile methods offer another promising strategy. For example, maintaining the structure of traditional military planning processes while incorporating Agile practices such as iteration, feedback, and adaptation can provide a bridge between approaches. These hybrid models recognise the reality that military organisations cannot completely abandon

hierarchical structures, but they can improve them with Agile principles. Leadership support and involvement are critical to successful Agile implementation. Leaders must not only support Agile adoption but also model the behaviours and mindsets that support it, including accepting appropriate levels of uncertainty, encouraging experimentation, and valuing learning from failure. Education and training programs should address both Agile technical practices and the underlying mindset shift towards adaptability and continuous improvement (Tudose 2021).

## 7. Future directions and research opportunities

### *7.1. Emerging trends in Agile adoption in the military*

Several emerging trends suggest growing interest and innovation in applying Agile methodologies in military contexts. These include integrating Agile with artificial intelligence and autonomous systems, extending beyond IT to operational domains, and developing military-specific Agile frameworks tailored to the unique requirements of military operations.

As military organisations increasingly use artificial intelligence, machine learning, and autonomous systems, Agile approaches provide valuable frameworks for managing these complex, rapidly evolving technologies. The iterative and adaptive nature of Agile aligns well with the continuous learning and improvement inherent in these technologies.

While many military Agile implementations have focused on IT and procurement projects, there is growing interest in applying Agile principles to operational planning and execution. Concepts such as agile command and control (C2) seek to increase adaptability in operational environments while maintaining the necessary command structures. These applications represent promising areas for future development and research (Orlov, et al. 2021).

### *7.2. Research and training needs*

Several research opportunities exist in the area of Agile adoption in the military. More empirical studies of military Agile implementations are needed to better understand outcomes and success factors in these specific contexts. Developing and validating military-specific Agile frameworks is another important area of research, as is investigating the cultural and organisational factors that influence Agile adoption in the military.

Training programs that address both Agile technical practices and the underlying mindset change are essential for successful implementation. They should be tailored to military contexts, recognising the unique challenges and requirements of military operations while preserving core Agile principles. Developing effective approaches to Agile education in military training institutions is an important area for development.

The intersection of Agile methodologies with military strategy and doctrine offers particularly rich opportunities for research and innovation. Exploring how Agile principles can improve military concepts such as mission command, commander's intent, and the OODA loop could provide valuable insights for both military operations and Agile project management (Schwaber and Sutherland 2020).

***7.3. Technology enablers for Military Agile***

Technological advances can support and enhance the application of Agile methodologies in military contexts. Digital collaboration tools working within security constraints can enable the application of Agile practices in geographically dispersed military units. Advanced analytics and decision support systems can provide the rapid feedback needed for effective iteration and adaptation in complex environments. Simulation and modelling capabilities can support experimentation and learning without the risks associated with real-world operations.

The military's increasing adoption of cloud computing also supports Agile deployment by providing more flexible and scalable environments for development and deployment. This shift to the cloud increases organisational agility by reducing reliance on outdated systems with limited flexibility.

These technology enablers, combined with appropriate organisational change and training, can help military organisations overcome some of the practical barriers to Agile implementation. By providing infrastructure and tools that support Agile practices, technology can facilitate the transition to more adaptive approaches to planning and execution (Orlov, et al. 2021).

## Conclusions

Applying Agile project methodologies to military action planning is a promising approach for improving adaptability and responsiveness in dynamic operational environments. Evidence from military IT projects and initiatives such as Diggerworks demonstrates that Agile methodologies can bring tangible benefits in terms of speed, quality and operational effectiveness. By adopting principles such as collaboration, iteration, and adaptation, military organisations can improve their ability to respond effectively to the complexity and uncertainty of contemporary operations.

However, implementing Agile methodologies in military contexts presents significant challenges, including organisational resilience, security requirements, and scaling issues. Addressing these challenges requires thoughtful implementation strategies that balance the need for adaptation with respect for the necessary military structures and processes. Hybrid approaches that combine elements of traditional and Agile methods offer practical paths forward, recognising organisational realities while pursuing significant improvements in adaptability.

As military organisations continue to explore and adopt Agile approaches, opportunities exist for further research, innovation, and development of military-specific frameworks. By learning from experiences gained in both military and non-military contexts, organisations can develop approaches that leverage the strengths of Agile while addressing the unique requirements of military operations.

In an era of rapid technological change and evolving threats, the ability to adapt quickly and effectively is increasingly critical to military success. Agile methodologies, which emphasise adaptability, collaboration, and continuous improvement, provide valuable tools for improving this capability and can contribute to more effective and responsive military operations in the 21st century.
The journey towards more agile military planning is only just beginning, but early results suggest that this path holds great promise for improving military effectiveness in complex and dynamic environments.

## References

**Abercrombie, Erick, Patrick Fullbright, and Seth Long.** 2016. *Analysis of the Marine Corps Supply Management Unit's Internal Operations and Effect on the Warfighter.* MBA Professional Report, Monterey, CA: Naval Postgraduate School. https://apps.dtic.mil/sti/tr/pdf/AD1030643.pdf.

**Agile Manifesto.** 2001. *Manifesto for Agile Software Development.* https://agilemanifesto.org/.

**Alaidaros, Hamzah, Mazni Omar, and Rohaida BT Romli.** 2021. "The State of the Art of Agile Kanban Method: Challenges and Opportunities." *Independent Journal of Management & Production* 12 (8). doi:10.14807/ijmp.v12i8.1482.

**Budden, Phil, Fiona Murray, Isaac Rahamim, Dylan Brown, and Nick Setterberg.** 2021. *Kessel Run: An Innovation Opportunity for the U.S. Air Force.* Mission Innovation Working Paper, Cambridge, MA: Massachusetts Institute of Technology. https://innovation.mit.edu/assets/Kessel-Run.pdf.

**Cebon, Peter, and Danny Samson.** 2012. *Diggerworks: Driving Innovation and Effectiveness in the Defence Sector – A Study of Success Factors.* Melbourne: University of Melbourne.

**Chung, Lawrence, and Brian Nixon.** 2013. *Mission-Oriented Agile Software Development.* Fort Belvoir, VA: Defense Technical Information Center.

**Daraojimba, Emmanuel Chibuike, Chinedu Nnamdi Nwasike, Abimbola Oluwatoyin Adegbite, and Chinedu Alex Ezeigweneme.** 2024. "Comprehensive Review of Agile Methodologies in Project Management." *Computer Science & IT Research Journal* 5 (1): 190-218. doi:10.51594/csitrj.v5i1.717.

**Kanban University.** 2021. *The Official Kanban Guide.* Seattle, WA: Mauvius Group Inc. https://resources.kanban.university/wp-content/uploads/2021/06/The-Official-Kanban-Guide_A4.pdf.

**Kniberg, Henrik, and Mattias Skarin.** 2010. *Kanban and Scrum: Making the Most of Both.* InfoQ Mini Book Series, C4Media Inc. https://www.agileleanhouse.com/lib/lib/People/HenrikKniberg/KanbanAndScrumInfoQVersionFINAL.pdf.

**Orlov, Evgeniy Vladimirovich, Tatyana Mikhailovna Rogulenko, Oleg Alexandrovich Smolyakov, Nataliya Vladimirovna Oshovskaya, Tatiana Ivanovna Zvorykina, Victor Grigorevich Rostanets, and Elena Petrovna Dyundik.** 2021. "Comparative Analysis of the Use of Kanban and Scrum Methodologies in IT Projects." *Universal Journal of Accounting and Finance* 9 (4): 693-700. doi:10.13189/ujaf.2021.090415.

**Rigby, Darrell, Jeff Sutherland, and Andy Noble.** 2018. "Agile at Scale." *Harvard Business Review.* https://hbr.org/2018/05/agile-at-scale.

**Schwaber, Ken, and Jeff Sutherland.** 2020. *The Scrum Guide: The Definitive Guide to Scrum: The Rules of the Game.* https://scrumguides.org/docs/scrumguide/v2020/2020-Scrum-Guide-US.pdf.

**Šmite, Darja, Javier Gonzalez-Huerta, and Nils Brede Moe.** 2018. "When in Rome, Do as the Romans Do: Cultural Barriers to Being Agile in Distributed Teams." *Blekinge Institute of Technology.* https://doi.org/10.1007/978-3-030-49392-9_10.

**Supriyadi, Arip, Moeljadi, Adi Kusumaningrum, and Susilo.** 2023. "The VUCA of Strategic Environment in the Defence Planning of Indonesian Marine Corps." *International Journal of Innovation, Creativity and Change* 17 (2): 40-52.

**Toroi, George-Ion, and Cristian-Octavian Stanciu.** 2023. "Aspecte privind planificarea acțiunilor de inducere în eroare la nivel operativ." *Gândirea Militară Românească* (nr. 3): 20-45.

**Tudose, Cătălin.** 2021. "Agile Methodology and War Strategies." *Journal of Systemics, Cybernetics and Informatics* 19 (8): 95-112. https://doi.org/10.54808/JSCI.19.08.95.

**U.S. Air Force.** 2019. *The Air Force is becoming more agile – one project at a time.* https://www.afmc.af.mil/News/Article-Display/Article/1823609/the-air-force-is-becoming-more-agile-one-project-at-a-time/.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

# Aspects Concerning the Training Process of Personnel participating in Multinational Operations

**Major Alice-Claudița MANDEȘ, PhD candidate***
*NHRM Structure / Joint Force Command, Military Science and Intelligence Field
"Carol I" National Defense University, Bucharest, Romania
e-mail: mandesclaudita@gmail.com

## Abstract

The ways and means by which the training of personnel participating in multinational operations is organized, planned and executed greatly influence the achievement of the objectives of the military actions in which Romanian military personnel participate, regardless of whether the multinational operation is conducted under the leadership of the United Nations (UN), the North Atlantic Treaty Organization (NATO), the European Union (EU) or the Organization for Security and Cooperation in Europe (OSCE). At the same time, the quality of the training process, the adaptation of the objectives of the selection stages to the specifics of the mission, to the degree of danger of the actions carried out and, last but not least, to the region of deployment of the multinational operation always represent synthetic benchmarks through which the success of the military operation can be determined.

**Keywords:**
multinational operations; mission objectives; quality standards; military personnel; military action planning; professionalism; professionals.

**Article info**
Received: 3 March 2025; Revised: 9 April 2025; Accepted: 13 May 2025; Available online: 27 June 2025

Citation: Mandeș, A.C. 2025. "Aspects Concerning the Training Process of Personnel participating in Multinational Operations. *Bulletin of "Carol I" National Defence University*, 14(2): 326-333. https://doi.org/10.53477/2284-9378-25-33

Military actions conducted in a multinational framework involve skills that are not necessarily a common part of general or specialized military training. Multinationality highlights not only the need to legitimize the military actions of multinational forces (Herciu 2019, 19). From this point of view, both NATO and the EU must be able to ensure full cooperation not only among the member states participating in the multinational operation, but also with other states contributing troops from outside their sphere of responsibility.

Therefore, the training for this type of action is specialized, which is somehow above the usual military training. The basic skills and principles for multinational operations differ from mission to mission; they are not similar for an Alliance-type mission or a coalition of forces, with only member states or with non-member states, respectively, a peacekeeping or peace enforcement mission, for example.

Along with the selection process, the success of the mission conducted in an international context largely depends on the way in which the training process for personnel participating in multinational operations is developed and implemented, which necessarily requires an understanding of the space for engaging forces and the complexity of the multinational operation (Herciu 2019, 21). In other words, the two processes make a significant contribution to quantifying the results of the multinational operation.

The two processes mentioned above, both the selection process and especially the training process that takes place after the completion of the first one, influence each other, are complementary, and value each other. A well-thought-out, efficient, and effective selection process shows us both how the selection should be carried out and how it can be better enhanced. Subsequently, the entire training process ensures the preparation of the selected soldiers for participation in the multinational operation, to the specifics of the mission, so that they can face the rigors, risks, and threats identified for the respective operation (Alexandrescu and Băhnăreanu 2007, 39-40).

## Organizing the training process

The process of training for personnel participating in multinational operations under the command of international security organizations contains a complex set of measures and activities that are organized, planned, and executed for the acquisition by military personnel of the knowledge necessary to carry out missions during deployment in the theatre of operations. As a rule, the process of training personnel for participation in multinational operations has an intensive, practical-applicable, multidisciplinary character, in order to carry out missions by the entire military force to high standards in safe conditions, as much as possible without unnecessary risks, with reduced resource consumption. In accordance with the new concept of training military personnel (Stoica 2015, 38) participating in multinational

operations, we believe that it is necessary to plan and organize their training based on a plan perfectly adapted to the mission conditions.

From a *temporal perspective and specific location*, the training process of military personnel taking part in military actions in theatres of operations covers two main phases, namely the one *intended for the preparation* of multinational missions, which is carried out predominantly within the unit assigned to carry out military actions of this type, through training programs and lessons where the emphasis is on knowing the standard operating procedures within the mission in which the military structure is to participate, on knowing the specific conditions in the country of mission, through advanced training and specialization courses, therefore a theoretical training, as well as through practical-applicative activities, exercises, various staff trainings, with a profound demonstrative and methodical character.

The materials presented during the theoretical training can be organized in the form of lessons that will have both presentations and practical sessions, always taking into account that the information necessary for the mission is obtained both through the effort of each participant (individual study), and through verifications regarding existing and possible situations that may arise in the theatre of operations, depending on the deployment area. The final result must aim at obtaining a volume of knowledge that will ensure that the mission participants fulfil the tasks received, resulting from the job description.

*The second phase* concerns the time spent in the theatre of operations, during the execution of the multinational mission, the training of personnel having a special note, in the sense that all this activity will be carried out in a decentralized manner, considering the sometimes-large distances that can separate the locations of personnel deployment within the same contingent, this being carried out according to necessity, situation and time available.

We consider the way in which the training activity is carried out, in the deployment area, in the theatre of operations, to be very important. In this regard, the continuous training process should take into account that the training sessions should have both a theoretical and a practical-applicative character, with the presentation of information and concrete situations, for which the allocation of time should take into account newly emerging aspects and, obviously, the elimination of some formal behaviours, generated by stationing in the theatre of operations for a longer period of time or by some events that influence the way the personnel act.

Due to these particularities, it is necessary that during the preparation of the mission, a minimum number of personnel should be selected to participate in a separate training program that will provide them with the knowledge necessary to conduct the specific training from both a theoretical and practical point of view, but especially a psycho-pedagogical one.

On the other hand, from the perspective of the *organization and planning of the learning process*, the training of all personnel participating in the multinational operation is of a special nature, and it must be carried out on two coordinates. Thus, *the first stage* represents the basic level of training (individual training stage) that all personnel and, within it, all military personnel must reach, regardless of the multinational mission in which they participate, regardless of the specialties and positions held. This stage aims to ensure the knowledge and skills necessary to execute multinational missions.

*The second stage* aims to achieve specific training (collective training stage), depending on the type of mission in which the unit is involved. We would like to highlight the fact that all training topics intended for both the entire staff and the staff performing various functions will be distributed progressively during the individual training stage, but also during collective training, aiming to accumulate the basic knowledge necessary for the mission, as well as the specific ones, adapted to the conditions of the geographical area of the mission and the theatre of operations.

## Specific elements of the training process

The training of personnel selected to participate in multinational operations is carried out differently, by personnel category, in relation to the category they belong to, and considering the functions that the military personnel are assigned to. Thus, from the perspective of understanding the situation and the context in which the multinational operation is carried out, a theme is considered that includes, among others:

- knowledge of the principles and requirements of the doctrine of joint multinational operations, of the organization and functioning of the security organization in command of the multinational operation, and their application to the achievement of general and specific objectives;
- improving knowledge regarding the management of military actions in a multinational framework, and cooperation with other units present in the theatre of operations;
- manoeuvring of forces and means of the structures in the theatre of operations, in relation to the missions received, ways of solving the problems that may arise, etc.;
- knowledge of the technical-tactical characteristics, construction, operation, maintenance, and repair of the equipment in the endowment, of the equipment received from various partners in the theatre of operations, including the principles of their efficient use;
- knowledge of the provisions of national regulatory acts and those contained in the SOPs of the multinational operation, relating to general and specific activities;
- the measures required during the preparation, arrival, and deployment of

the mission regarding ensuring the actions and protection of personnel and equipment, own materials, knowledge of recognition signals, implementation of the information system, etc.;
- knowledge and application of specific work measures and safety rules, and technical supervision of pressure and lifting installations, measuring instruments, as well as fire prevention and fire extinguishing measures;
- knowledge about how to ensure connections, gather information, prepare and present information reports to the country, respectively to the regional command, etc. (SMG/Ctr. 1 2008, 41-46).

Very important is the way in which the commanding officers of the structure that is to move to the theatre of operations understand how to ensure the training of the personnel in relation to the specific aspects of all functions. Thus, if for the technical personnel, the military personnel who receive and are responsible for the operational status of the military equipment, practical-applicative sessions are usually organized and carried out regarding the specific ways of conducting maintenance and repair works, respectively, with the personnel responsible for ensuring campaign services or operational medical support, the introduction of training sessions will have to be considered that highlight the way in which the relationship is achieved with the structures responsible for logistical support in the theatres of operations, while with the military personnel who form the manoeuvre units (platoons, groups, etc.), the concrete ways of action, communication, cooperation and collaboration during the execution of military actions of an operational nature are presented and practiced.

Theoretical and practical-applicative training sessions are organized and carried out, as a rule, both during the time allocated to specialized training and during the periods intended for the preparation of exercises or other specific activities, depending on the destination of the structures within the unit (subunit) taking part in the multinational operation.

In this regard, it is worth noting that, for the personnel who enter the composition of the unit (subunit) through detachment, separate training sessions must be considered for understanding the role, place, and mission of the structure that is to be deployed in the theatre of operations. From this perspective, the sessions can be carried out in a differentiated manner, depending on the positions held in the organizational state by the respective military personnel.

The following remark should also be made here. Situations quite often arise in which new categories of equipment and technology are introduced into the units (subunits) participating in multinational operations, even during the preparation for the mission. In this case, as a rule, the training of those who will operate the equipment and technology is carried out both during the preparation of the mission (depending on the remaining time available), and later, after deployment into the theatre of operations. In such situations, a decision can be made to intensively train some of

the detachment's servicemen, with the experience they have gained subsequently being shared with the others.

Given that, during the second stage, specific training for the conditions of the theater and the mission area is taken into account (the collective training stage), during this type of training, emphasis can be placed not only on training personnel through field exercises, but also on the training, specialization and improvement of military personnel in the context of receiving new categories of equipment and technology, in accordance with the provisions of the regulations developed at the level of the Defence Staff and the categories of forces, for newly emerging situations.
The commanding officers of the units to be deployed in the area of operations are responsible for the way in which the training process is organized, planned, and executed in order to learn how to operate the new equipment, respectively, for updating the content of the materials used in the training process.

Last but not least, commanders of structures (units, subunits) participating in multinational operations should consider the fact that the personnel training process must ensure not only general knowledge of the nature of the missions to be executed, but it should also allow, through a modern approach, an accurate understanding of the actual way of executing them. Thus, all personnel must obtain and possess, during the execution of the mission, the skills that allow them to behave coherently in a multinational force structure, which must act based on the trust of the local population and its acceptance of its mode of action (based on standard operating procedures).

A great responsibility pertains, in the context of the participation in the multinational operation of the Romanian staff and force structures, to the specialized structures within the Defence Staff and the categories of forces, respectively the support commands, for the development of regulations and concrete instructions regarding the training of Romanian military personnel in such multinational operations, to the way in which they ensure the monitoring and verification of the acquisition of the initial and final capacity for action. In this regard, they will have to ensure that the participating military personnel obtain at the end of the training process the necessary knowledge for the successful accomplishment of both the individual missions, specific to the positions occupied, and the collective one, depending on the objectives of the multinational force.

Thus, all personnel participating in the multinational operation should be able to understand and apply the standards of the international security organization in command of the multinational operation, the existing procedures at the level of the multinational force, but also the national ones in activities regarding the organization, financing and administration of own resources and those made available by NATO, EU, UN or OSCE, respectively the specific way of negotiating and entering into contracts in the theater of operations or to obtain certain resources from the country

considered the Host Nation for the multinational force (fuel, lubricants, drinking water or for household needs, temporary accommodation and quartering facilities, class I materials and products, labor, other field services).

## Conclusion

Through what has been presented, we wanted to review the manner how the training process of military personnel participating in multinational operations is carried out, which leads us to the idea that this type of approach has a fairly significant generality, meaning that it can be very easily applicable to military structures (units, subunits) with different specificities and fields of activity.

Given that the training process does nothing more than practically complete the selection process, we believe that, for the future, the two should be analysed in an integrated manner, without having differences in terms of approach. On the other hand, we believe that the organization and planning of a training process should not lose sight of the concrete ways in which the acquired knowledge must be refreshed periodically. This approach would be a continuation of the two processes already mentioned, ensuring a series of new training methods, proposing concrete paths of action, as well as tools, through which the acquired knowledge is periodically brought back to the attention of the military participants in the multinational operation.

Organizing training sessions, during the execution of the multinational mission, without a long duration, with a certain intensity, administered in a pleasant manner, can contribute to recalling the information and data presented during the training period in the country, to the memory of the soldiers.

From the perspective of the lessons identified and, subsequently, those learned, it became very clear that the management, planning and implementation of a judiciously formulated training process can come to the aid of the military participants in the multinational operation, being not only a proof of professionalism of the management and execution bodies at the level of the military structures involved, but also a measure by which a series of undesired events involving both personnel and modern technology and equipment can be avoided.

We support this idea by the fact that the implementation of an appropriate training program can not only contribute to the elimination or minimization of some shortcomings in current activity, but can also lead to an increase in the combat capacity of units taking part in multinational operations, to the avoidance of most of the outages of their own equipment and technology, as well as to the increase in the average uptime and, implicitly, the degree of serviceability of the equipment deployed in the theatre of operations.

From the perspective of what has been presented, it becomes obvious that the success of the military actions of the Romanian Army structures participating in multinational operations within NATO and the EU depends to a large extent on both their self-sustaining capacity in the theatres of operations, and especially on the combat potential (Moldovan 2007, 50), acquired following the completion of the selection and training processes by the military personnel who comprise these structures.

## References

**Alexandrescu, Grigore, and Cristian Băhnăreanu.** 2007. *Expeditionary military operations.* Bucharest: Publishing House of the National Defense University "Carol I".

**Herciu, Alexandru.** 2019. „The physiognomy of the joint multinational operation." *Bulletin of the "Carol I" National Defense University* (Publishing House of the National Defense University "Carol I") 6 (3): 14-21.

**Moldovan, Dorinel-Ioan.** 2007. "Priorities of integrated management of defense resources regarding international missions." *Integrated management of defense resources. Necessity, current affairs, perspectives (session of scientific communications).* Brasov: Publishing House of the Regional Department of Studies for Defense Resources Management.

**Parliament of Romania.** 2011. "Law no. 121 of June 15, 2011 on the participation of the armed forces in missions and operations outside the territory of the Romanian state." Published in the Official Gazette no. 427 of June 17, 2011.

**Romanian Defense Staff.** 2014. *Personnel Support Manual in Operations.* Bucharest.

**SMG/Ctr. 1.** 2008. "Instructions regarding the combat evaluation of the units/detachments from the land forces participating in missions outside the territory of the Romanian state." Bucharest.

**Stoica, Viorel.** 2015. „Reserve forces and the mechanism for replenishing losses in military actions." *Bulletin of the National Defense University "Carol I"* (Publishing House of the National Defense University "Carol I") 2 (3): 34-40.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS


**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: 26.06.2025
The publication consists of 334 pages.

410/26.06.2025

C.160/2025