BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 3/ 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. 3/2025

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

"Glorious Past, Age-Old Connection with Russia" Moscow and the Russo-Moldovan Historical Ties

Independent Military-Political Analyst, Nico LAMMINPARRAS*

*MA, Doctoral Researcher/University of Helsinki, Finland
e-mail: nico.lamminparras@gmail.com

Abstract

The article delves into the Russian assessment of the common Russo-Moldovan past, pronounced in the framework of the Moldovan EU referendum and the concurrent presidential elections in October-November 2024. Discourse analysis, as defined by Ricoeur and Fairclough, is applied to the public speeches of Maria Zakharova, the spokesperson of the Russian Ministry of Foreign Affairs. Occasionally, these are triangulated with the articulation of the Russian president, Vladimir Putin. However, due to her frequent appearances concerning Moldova, it is Zakharova who represents Russia in this issue. Entirely, Moscow's discourse on Moldovan history is tackled within the frames of the Russo-Moldovan past and present.

With a confrontational approach, Zakharova slams the Moldovan EU referendum for having taken place under totalitarian circumstances. It was the West that plotted to convert Moldova into a NATO base. The Moldovans dismissed this course since they cherish their history and their centuries-long bond with Russia. As does Putin, the spokesperson, who oversees 1200 years of Slavic-Romanian encounters. While Zakharova recaps Russia's impact on Moldova's uniqueness from the 18th century to the Soviet era, she applies a descriptive representation of facts. Hence, she covertly exhorts the Moldovans to impede the country's further integration in the West. Yet, Zakharova is unable to overcome the perpetual paradoxes throughout the ages – the similarity of Moldova and Romania, the constant economic decay, and the permanent Russian hegemony.

Keywords:
Russia; Moldova; Maria Zakharova; History; Bessarabia; MASSR; MSSR; Discourse Analysis.

Article info
Received: 1 July 2025; Revised: 4 August 2025; Accepted: 2 September 2025; Available online: 6 October 2025

Citation: Lamminparras, N. 2025. "Glorious Past, Age-Old Connection with Russia" Moscow and the Russo-Moldovan Historical Ties." *Bulletin of "Carol I" National Defence University*, 14(3): 7-28. https://doi.org/10.53477/2284-9378-25-34

On October 20, 2024, the Moldovan referendum on EU integration – or technically, on the constitutional amendments to outline the EU as the country's strategic objective – turned into a spectacle. Even if the preliminary results attested a clear rejection of the changes, the following dawn, the approval of the constitutional reform obtained a majority of a few hundred ballots. Then, the gap only increased. Numerically, the outcome turned 50,35 percent in favor of the amendments, while 49,65 percent voted against the changes (CEC 2024a). It is pertinent to note that the plebiscite was conducted side by side with the first round of the presidential elections. The incumbent pro-Western Maia Sandu obtained 42,49%, and Alexandr Stoianoglo, considered as her prime opponent, gathered 25,95% percent. However, if all the candidates, whether moderately or staunchly pro-Russian, are calculated, the Eastern orientation as such was desired by 51,5 percent (CEC 2024b).

Substantially, both these outcomes reiterate the thesis of Sergeyev a decade ago. The conflict in Moldova since the late perestroika is not about ethnicity or nationality, rather, it is a confrontation of two larger perceptions on heirloom. While the pro-Romanian élite of Moldova stands for the Latin roots, it simultaneously promotes the country's age-old Europeanism. Contrastively, the Russian-speakers (those who prefer Russian as their first language) view themselves as an inalienable part in the string of Slavic generations – or more exactly, the Russian World (Sergeyev 2015, 13). As for Southern Moldova, or Gagauzia as it came to be known, the causes and the evolution of the confrontation prove similar. The visible exception is the yet unfinished dispute on the ethnogenesis of the Gagauz (Bejan 2022, 29–38, 224–225, 229–238).

Russia was to first address the referendum and the elections on October 21, 2024. On one hand, to track the contiguous themes, on the other, to discover the plausible alterations in Moscow's standpoint, I have extended the research period until November 28, the same year, i.e., to the date of validating the results of the presidential elections (CCM 2024). Markedly, it is the spokesperson Zakharova to pronounce Moscow's positions on Moldova, not President Putin nor the Minister of Foreign Affairs, Sergey Lavrov. A search with the voice 'Молдова' (Moldova in Cyrillic) reveals this. During the timeline from January 1, 2024, to the date of finalizing the text, August 26, 2025, the Kremlin's search engine returns only four results with the voice (Kremlin 2025). These locutions consist of a one-word mention of the country; one of them is not even pronounced by Putin himself. In Lavrov's case, the results in the MFA's search engine total ten within an equal timeframe. Notably, the latest one dates as far as January 2025 (MID-1). As for Zakharova, the number is overwhelming, 59 results (MID-2). Therefore, with solid grounds, one may state that Zakharova incorporates Russia in Moldovan issues.

With the topical commentaries and briefings after the presidential run-off on November 3, the number of sources is seven. Regarding the campaign phase and the polling day, Zakharova underscores the undemocratic circumstances that reigned

during the electoral process, with open allusions to the "repression" of media and of those dissenting from the European alignment. The 300 to 500 thousand Moldovans residing in Russia were practically deprived of the right to express their will, whereas the utmost slight majority was obtained through "a mobilization" of the equally large diaspora in the West. These allegations were destined to defame Moldova, and thus, to hamper its pro-European course (Lamminparras 2025, 35, 38–40, 42–43). Moreover, the spokesperson retains diplomacy both as a struggle and as an unsolicited movement (Kireyeva and Pikuleva 2019, 22–24). Accordingly, the final purpose of all the Western "meddling" was to rip Moldova off its sovereignty – and under the disguise of the EU, to transform it into an anti-Russian NATO stronghold (Lamminparras 2025, 40–42, 43).

Suddenly, the Moldovans within the boundaries of the republic hoisted "a non-confidence vote" against Sandu and her government (Zakharova-K04N 2024). 54,6 percent voted against the constitutional changes. The figure for the Moldovans with residence in Pridnestrovye was 69 percent, and for the Gagauz, just short of 95 percent (CEC 2024a). It is worth noticing that the Gagauz opinion appears firm. Ten years earlier, the same percentage rejected EU integration (Romanova 2022, 497). I invite my fellow scholars to deepen this preliminary investigation. Altogether, the suggestion of Sergeyev on the "two worlds" not only persists but is utterly tangible. This understanding was warmly welcomed by the Russian MFA: the premeditated fraud did not deceive the local people. According to Moscow, the reason proves simple but fundamental. Already, the Moldovans are in Europe: "through their labor and history they have made a colossal contribution to the European civilization" (Zakharova-B21N 2024). Therefore, the Moldovans are proud of their magnificent past, and they especially value the age-old tie with Russia (Zakharova-B30O 2024). Regrettably, all these are threatened by one of the prime Western instruments of interference, that is, "the obliteration of Moldova's national identity, language, culture, and history" (Zakharova-K21O 2024). In contrast, it has been precisely Russia that has both enhanced and preserved the uniqueness of Moldova. To illuminate and advocate this vital mutuality, the spokesperson delivers a lengthy historical account (Zakharova-B30O 2024).

The emphasized recurrence to history is in line with the law 'On the Fundaments of the State Policy of the Russian Federation within the sphere of Historical Enlightenment' (Osnovy 2024), promulgated by Putin in May 2024. Therefore, to disentangle the strategic narratives and potential discrepancies in Moscow's stance on Moldova's past, it is imperative to explore Zakharova's language and communication. Throughout this inquiry, the textual and sociocultural levels of discourse analysis, as outlined by Fairclough, are applied to the public speeches and statements of Maria Zakharova. According to Fairclough, there are three levels of discourse analysis. As the name "textual" reveals, the first one focuses on solitary enunciations and word choice. The second level – "production" – considers resources and procedures behind any text or presentation. On the third level, which perhaps is the most

challenging, a scholar tends to differentiate the social and cultural suggestions of a given presentation (Fairclough 1992, 1, 38, 62–63, 87). To simplify these links, the substance of the words emerges from the framework in which they occur (Eskola 1996, 65, 127); therefore, a complete axiom refers "beyond itself" to the (semantic) society in question (Ricoeur 1976, 6–7, 20). In total, I distinguish the expressions, implications, and gaps of Zakharova's articulation. The auxiliary questions are:

- How does the spokesperson depict the Russo-Moldovan ties?
- How does the sociopolitical environment shape Zakharova's utterance?
- What questions does Zakharova remain tacit on?

The translations from Russian, Romanian/Moldovan, Finnish, Estonian, and French are produced by the author of the current text. Inasmuch as to assist the readers in tracking the history behind the events, to avoid repetition, the chapters are thematically organized. In connection with the Moldovan parliamentary elections on September 28, 2025, this article is a valuable product of a scientific research effort and serves, in addition to general information and background, for this purpose.

Despite official claims of Moldova's distinctiveness, the probe exposes a series of divergences between stated policy and factual approach. Zakharova gladly offers detailed figures concerning the boost that Russia has brought throughout the centuries in the faraway region. Thus, she clandestinely encourages the Moldovans to encumber the country's pro-Western integration. Logically, Zakharova remains silent on those episodes that rather accentuate the resemblance between Romania and Moldova. Also, to evade any debate on the era of stagnation, Zakharova finishes her educational and economic accounts on Bessarabia in 1860-1861. These times would merely compromise the core objective of Zakharova's narration – to exhort the Moldovans to cherish the age-old ties with Moscow.

1. Research tools

This section is to clarify the acronyms and abbreviations utilized throughout the text. The source material is readily explained above. To conclude this section, I will discuss the findings of my predecessors.

1.1. Acronyms

EU	European Union
KASSR	Karelian Autonomous Soviet Socialist Republic (1923-1940)
KSSR	Karelian Soviet Socialist Republic (1940-1956)
MASSR	Moldovan Autonomous Soviet Socialist Republic (1924-1940)
MFA	Ministry of Foreign Affairs (RU)
MID	Ministerstvo inostrannykh del (Pridnestrovye)
MSSR	Moldovan Soviet Socialist Republic (1940-1991)
NATO	North Atlantic Treaty Organization
Osnovy	Foundations of the SPRF within the sphere of Historical Enlightenment

PMR	Pridnestrovskaya Moldavskaya Respublika (Pridnestrovye)
SPRF	State Policy of the Russian Federation
USSR	Ukrainian Soviet Socialist Republic (1918-1991)
USSR	Union of Soviet Socialist Republics (1922-1991)

1.2. Literature review

There are plenty of pages on (Romanian-)Moldovan history, with their focus ranging from the primeval ages to contemporaneity (Eyal and Smith 1996; Bruchis 1996; Bărbulescu, et al. 1998; King 2000; Dima 2001; Skvortsova 2002; Negru 2003; Roper 2008; Lamminparras 2014a; ibid. 2014b; Sergeyev 2015; Babilunga 2015; Dulgheru 2016; Dulgheru 2018; Ţicu 2019; Bejan 2022; Negru Gh. 2023; Negru E. 2023). While all these, to a notable extent, tackle the Russian imprints throughout Moldova's history, its culture, etc., analyses with a specific accent on Moscow's corresponding speak constitute a rarity (for instance, Lamminparras 2024a). As previously mentioned, the primary Moldova commentator in Moscow is Maria Zakharova, not President Putin nor the Minister of Foreign Affairs Lavrov. Maybe due to the language barrier, most of the investigations on Zakharova's discourses are conducted in Russia, or by Russian-speaking academics. Since many of these date to the pre-war days, this examination renews and augments our topical information.

First, as noted by Gorbacheva and Zaynullina, Maria Zakharova is the first female to serve as the head of the Department of Information and Press of the Russian MFA [spokesperson]. She was nominated for the post in 2015. One of her core virtues is that she does not limit herself to the regular communication channels. Zakharova is famous for her appearance on TV talk shows and on social media platforms (Gorbacheva 2016, 7; Zaynullina 2018, 166; see also Martynenko and Mel'nikova 2016). Another factor in her popularity is her clear and sharp tongue, combining ironic notions, detailed narration, and insurmountable facts. Consequently, the spokesperson has become one of the most cited Russian diplomats, or to be exact, "the main media face" of the MFA (Kireyeva and Pikuleva 2019, 21).

During the last years, Zakharova's utterance has drawn wider attention. The obvious reason is the all-out war in Ukraine, on which Zakharova comments in harsh language, especially about the sufferings in Donbas (see, e.g., Belova-Dalton 2023, 69, 77, 80). Somewhat paradoxically, Sandler holds that Zakharova possesses various communicative resources under the setting of a fierce military-political and cultural-ideological confrontation between the Russian World and the collective West (Sandler 2022, 116). In general, Sandler explores the diverse techniques and strategies the spokesperson employs, such as an explanatory nature and diplomacy as a struggle. Most recently, I probed Zakharova's discourse on the Moldovan EU-referendum, but from the (geo)political point of view. The spokesperson defames Chisinau by condemning the plebiscite, which has been conducted through numerous violations of basic civil and human rights. This stark notion is to impede the country's pro-EU course. As does President Putin, so does Zakharova kindly

relate to the ordinary Moldovans and warn them of the consequences: in the European Union, their sovereignty would be lost. However, it is not the EU itself to endanger independence. Rather, a sizable electoral rigging was undertaken by the Western states for one single cause – to ultimately draw Moldova into NATO (Lamminparras 2025).

2. Lutsk alliance

Simply overlooking 1200 years, Zakharova begins her account from the early 18th century, as if there were no prior Russo-Moldovan contacts. Like President Putin, she bypasses the Slavic settlements in the areas today perceived as Romania, Moldova, and Bulgaria from the fifth to seventh centuries. Alike, she omits the Kievan Prince Svyatoslav's realm by the Danube in 969–971, the Medieval dynastical relations, and the alliance between Moldavia and the Muscovite crown in 1656. (For Putin's silence, see Lamminparras 2024a, 108–110, 112.) Ostensibly, these phases would testify to Fundament 5 of the Osnovy on the shared past and space. In its words, Russia comprehends "a mighty nation with hundreds of years of history, of state-civilization, which unites Russians and many other nations within the Eurasian plateau to one cultural-historical community" (Osnovy 2024). The likely explanation of Zakharova's omission seems to be the misfortunes of all the pre-1700 occasions; the early Slavic reigns along the Danube soon collapsed, and the later treaties were virtually never realized.

Whilst Zakharova applied a rather confrontational stratagem regarding the electoral circumstances – with a metaphorical model of diplomacy as a struggle, or a sheer war, she here shifts to the so-called descriptive representation of facts (Zakharova and this strategy, see Gorbacheva 2016, 9–10). As for the origins of the Russo-Moldovan interaction, Zakharova sets sail from the Moldavian Prince Dimitrie Cantemir:

> -- since the era of Prince Dimitrie Cantemir, Russia has constituted a trustworthy ally, played an important role in the preservation and development of the Moldovan statehood and national identity (Zakharova-B30O 2024).

Neatly, in the aftermath of the Battle of Poltava – with the joint Cossack-Swedish army defeated – King Carl XII and hetman Ivan Mazepa had fled to the Ottoman Bender by the Dniester. (Linnarsson 2022, 8–9; for Poltava, see, e.g., Englund 1988; From 2007). There, Mazepa soon died. Yet, his successor, Philip Orlyk, and the Swedish king prepared a new onslaught into Russia. The plan was leaked to Czar Peter I, which led to Dimitrie Cantemir's ascension to the Moldavian princely throne. However, like his predecessor, Cantemir aspired for the freedom of the Ottoman vassal principalities of Moldavia and Wallachia (Babilunga 2015, 31–32). Also, Cantemir projected a monarchical constitution instead of the boyar rule (Bărbulescu et al. 1998, 273–274).

The alliance was forged in Lutsk in April 1711. As stated by Babilunga, Peter I agreed to guarantee Cantemir's objectives (Babilunga 2015, 31–32). In this respect, Russia indeed progressed the Moldovan state formation and its identity, as Zakharova insists (Zakharova-B30O 2024). Although it does not foil this assumption, it is still valid to ponder whether Peter's benevolence was to endure or, to temporarily create an incentive for the Christians south of the Danube to align with Russia. Not least, because the alliance envisioned a Moldavia with its Medieval boundaries, i.e., with those dating to the era of Prince Ştefan cel Mare (Stephen the Great) in 1457-1504 (Dulgheru 2016, 159, 164).

However, Zakharova remains tacit about this aspect of the Treaty of Lutsk. She seems to be siding with Putin, who avoids these episodes, too. Apart from condemning Mazepa as a "mutineer", the Russian president speaks no word on this era (Putin 2021). The motivation is clear; any in-depth reference to Lutsk would only constitute a precarious precedent. If the borders were demarcated by the late 15th-century maps, the pro-Moscow republic east of the Dniester, Pridnestrovye, would lose Bender, its stronghold-entrance just on the western bank of the same river. Ukraine would have to relinquish its southwestern corner, the classical Basarabia (the western half of the modern Odesa region by the Black Sea), to Moldova. On the other hand, Chisinau could no longer claim the area east of the Dniester. During Ştefan cel Mare's epoch, Bender functioned as the princedom's eastern customs and border checkpoint. This triple territorial paradox looms as the probable cause for both Moscow and Chisinau's (and Kyiv's?) quietness.

Practically, the alliance fell in July 1711, as the Russian and Moldovan forces encountered the Ottoman army in Stănileşti, just west of the river Prut. Even though the result is described as undecided, Peter I renounced the Azov fortress and withdrew from Moldavia, followed by Cantemir (Babilunga 2015, 31–32). Exiled, Prince Cantemir developed Russian cartography, arts, and science. Alike, he served as Peter's right-hand aid (Dulgheru 2016, 159). Now what Zakharova misses, or purposefully omits, is Cantemir's conviction. Throughout his life, the prince advocated the Roman legacy and promoted the Latin heritage of his kinsmen (Ţîcu 2019, 88–90). Even if Cantemir nominally spoke of the Moldovans, substantially, he saw no difference between the terms 'Romanian' and 'Moldovan'. This, in turn, enters into a stark contradiction with Zakharova's utterance on a separate "Moldovan statehood" and a distinct "Moldovan national identity" (Zakharova-B30O 2024).

The paradox is analogous to the one President Putin barely avoids in his Moldova discourse (Lamminparras 2024a, 110–111, 112). If the MFA's spokesperson disclosed Cantemir's life's work, she simultaneously would highlight the common Romanian-Moldovan ancestry. Time and again, this would frustrate Moscow's claims on a unique Moldova and on its apparent proximity to Russia.

3. Bessarabian bloom

The following hundred years, Russia, as well as Austria, constantly engaged in wars with the Ottoman Empire over the Balkans (see, e.g., Lamminparras 2024b, 169–173, 182–183). The heyday of Moldova is the 19th century, as Zakharova introduces:

> After the signing of the Bucharest peace treaty in May 1812, the territory between the Dniester and the Prut, i.e., Bessarabia, was incorporated into the Russian Empire. From this hour, the revival of the Moldovan lands, devastated by the war, embarked (Zakharova-B30O 2024).

Foremost, the spokesperson continues her descriptive approach, with additional narrative markers, namely 'After' and 'From this hour'. Likewise, the positive description seems to echo one of the objectives of the Foundations of the State Policy of the Russian Federation within the Historical Enlightenment. Namely, it is "the formation of the [universal] Russian civil identity and the solidification of the community of the Russian world, founded on the traditional Russian spiritual-moral and cultural-historical values…" (Osnovy 2024). Since it was Russia that was to rejuvenate the new territory, logically, Bessarabia back then welcomed, and still embraces, the same ideals.

Yet, Zakharova's historical account circumvents a few elements. For example, the peace treaty obliged Russia to withdraw from the centuries-old principalities of Wallachia and Moldavia. It is worth weighing whether this outcome satisfied the emperor and his generals. Already by 1810, there was a plan to annex the Danube Principalities and to restructure these into four *oblasts* (provinces). The Ottoman resistance, the objections of the Great Powers, and the threat of Napoleon's invasion contributed to the constant revisions of the plan. Finally, "the worst-case scenario" was realized, and Russia had to contend with the area from the Dniester to the Prut (Bejan 2022, 84–85).

As depicted by Dulgheru, Czar Aleksandr I annexed the whole territory and "baptized" it as Bessarabia. Thus, the Czar distorted the original concept of Basarabia (Dulgheru 2016, 172, 174). Per se, the term 'Basarab' may have referred to Cumans who in the 11th century settled in the narrow shore strip from the Dniester to the Danube, today the western wing of the Odesa region. Bejan suggests that the nomination persisted for centuries since Basarab I, the Wallachian ruler who conquered the region in the mid-14th century, himself had Cuman origins (Bejan 2022, 58–59). As of 1812, the reshaped Bessarabia covered 45,360 km², but the estimates of its population vary from 350 to 500 thousand. Regardless of the exact number, more than eight out of ten spoke Romanian as their native tongue (King 2000, 20; Dima 2001, 14; Roper 2008, 80).

Conversely, Alexandr I's tolerant policy favored the bloom. The vast privileges of the local boyars, the status of the Romanian idiom, and the autonomy of the

[Orthodox] church were all guaranteed in 1818 (King 2000, 22). Bruchis insists that the true intention of the Czar's liberalism consisted of a showcase. That is, the vast freedoms of Bessarabia ought to attract Christians from the Ottoman Balkans (Bruchis 1996, 11). At the same time, this satisfied the local magnates (King 2000, 21–22). Following this interpretation, the Czar's objectives would only have repeated those of Peter I (the Great) a hundred years before. Nevertheless, an illuminating parallel is Finland, which the very same Czar Alexander had conquered four years earlier. In March 1809, Finland was granted the status of an autonomous Grand Duchy. The most significant turned out to be Alexander's assurances to maintain the Swedish-era laws, the prior privileges, as well as the language. Pragmatically, the language barrier alone in both fresh autonomies – Bessarabia and Finland – compelled the new potentates to resort to the local administrators. From a cynical perspective, none of these justifications proves exclusive. Due to the practical prerequisites, the Czarist regime took advantage of the ethnic people in the Northwest as well as in the Southwest, which indeed was liberal at its time. At once, this reflected the interests of the native élites, averting any plausible resentment, and conveyed an encouraging message about the new ruler.

If one follows Zakharova's articulation, the parallels do speak for each other. E.g., the boost the Russian rule embarked on in Bessarabia was overwhelming. From 1812 to 1917, the population increased 7.5-fold. Moreover, judging by the first nationwide census of 1897, Bessarabia ranked as one of the most inhabited territories of the empire (Zakharova-B30O 2024). Though it is questionable whether the demographic growth widely originated from within or from other Russian regions. As Eyal & Smith state, the so-called Novorossiya policy, i.e., resettlement with various nationalities, was promptly expanded into Bessarabia. The Jews were exempted from the military service and adorned with extraordinary rights, the Bulgarians and the Gagauz gained land ownership and economic privileges for three to seven years, and the Russians controlled the largest estates (Eyal and Smith 1996, 224; Bejan 2022, 89–91).

The heavy immigration explains the sizable increase of Bessarabian lands under crop cultivation and of those under viniculture between 1814 and 1861; the boom of their production, not to mention. Although Zakharova's description here is punctual, with exact figures included, she does not speculate or muse on the larger picture (Zakharova-B30O 2024). Repeatedly, if she extended her account, it likely transformed into a shaky history. Puzzlingly, the Russian rule did catalyze the development of the empire's southwestern frontier – but unlike in Finland, it was non-native folks who made it come true.

Second, what strikes the eye is the year 1861, in which Zakharova concludes her agricultural history of Bessarabia. There exist certain grounds to presume that the omission is dictated by the detrimental reform of the given era, especially within farming. After the Emancipation Reform of early Spring 1861, it is estimated that the arable land available for the freed serfs diminished by 18 percent. As for the fertile

soils in the entire South, the drop may have risen to 40 percent. At the time of the reform, 28 percent of the peasants could not ensure their subsistence. As the price for land kept increasing, in forty years this figure rose to 52 percent (Jussila 2006a, 240–241). Also, St. Petersburg's conservative policy and Czarist reactionism during the 1860s–1870s effectively hampered the first phase of modernization (Ţîcu 2019, 148). By remaining tacit on the latter half of the century, Zakharova evades launching a risky discussion on the dramatically altered rural circumstances in Bessarabia (and in the southern lands of the empire in general).

4. Educational evolution

The very same dilemma shapes Zakharova's claims on Bessarabia's cultural development. According to the MFA spokesperson, both the level and the volumes of education progressed:

> In Chisinau, a theological seminary was opened (in 1813), and besides that, a lay boarding house (in 1816). Till the year 1860, there operated 400 schools of all categories in Bessarabia, in which more than 12 thousand pupils were educated (Zakharova-B30O 2024).

In a peripheral region where the majority lived in rural areas and were illiterate (Ţîcu 2019, 98), such measures did stimulate civilization. Another encouraging factor may have been the initial schoolbooks, especially those compiled in the very region (Zakharova-B30O 2024).

Probably, the Russian occupation of Wallachia and Moldavia in 1828-1834 enhanced the national revival since it temporarily lifted the boundary drawn in the Prut. Not least, because the idea of the Moldovans as a separate nation first saw daylight in the 1840s. King underscores that the concept stemmed from the local people, though (King 2000, 26). Hence, to some degree, it is pertinent to state that the Russian Czardom factually provided for the "Moldovan statehood" and its "national identity" (Zakharova-B23O 2024). Save that it was a collateral, rather than an envisaged, outcome. On second thought, the self-perception of the very local people proved ambiguous. Up till the early 1860s, even the oblast's administration confirmed the inhabitants to identify themselves as Moldovans and/or to speak Romanian (Ţîcu 2019, 112–113).

Once again, Zakharova's narration ends in the early 1860s. This likely derives from the volatile czarist policy in Bessarabia. In 1821–1829, the political upheavals abroad sealed the fate of the region. The Greek Independence War and the brief revolts in Wallachia and Moldavia had dazed Saint-Petersburg, committed to safeguarding the balance in Europe. After the peace treaty with Persia, Russia in 1829 declared war against the Ottomans and expanded to the Danube. Moldavia and Wallachia gained autonomy under the Czar's protection (Jussila 2006b, 228–229).

Paradoxically, as the freedoms of the two Principalities augmented, those of Bessarabia were reduced. The constitution was abolished in 1829, which turned the region into an oblast (province) (Dima 2001, 14). While the unsuccessful Crimean War in 1853–1856 compelled Russia to withdraw from the shores of the Danube, which the empire lost for 22 years, the great powers guaranteed the autonomy of Wallachia and Moldavia. Repetitively, with the kinsmen's position strengthened, the Czarist regime tightened its grip on Bessarabia. For instance, Russian was decreed the official language in 1854 (King 2000, 22). Similarly, the unification of the Danube Principalities on January 24, 1859, under Alexandru Ioan Cuza, and the subsequent state-building of modern Romania (for the merger, see Bărbulescu, et al. 1998, 374–380) only accelerated the russification of Bessarabia. By the end of the decade, the Russian language had overpowered the educational institutions and government agencies in the oblast (Yekelchuk 2008, 14; russification of the Bessarabian educational system, see, e.g., Negru Gh. 2023).

Thus, if Zakharova furthered her articulation on "facts, the true history of the Moldovans" (Zakharova-B30O 2024), she would fall into a double trap. First, how to explain the paradox of Russia having enhanced the uniqueness of 'Moldova' whilst the dwellers saw no distinction between themselves and the brethren beyond the Prut and the Danube? Second, if the then-Bessarabian people were as diverse as alleged, why was their freedom relegated in concomitance with the political development in Wallachia and Moldavia?

5. Soviet society-engineering

By October 1917, various military and civic circles succeeded in forming a national assembly, which on December 2, 1917, declared Bessarabia autonomous (Yekelchuk 2008, 18–19). Again, the parallel proves Finland. The declaration outlined the region to remain within a reformed Russia, but its rights to be equal to those Finland enjoyed as a Grand Duchy (King 2000, 33). Likewise, the assembly elected the *Șfatul Țării* (Yekelchuk 2008, 19), literally the "Council of State", that is, the first Bessarabian government. According to Dima, from the very first hours, it was evident that Bessarabia would join Romania (Dima 2001, 17). However, King notes that the refugees from Transylvania, Banat, and other Romanian areas contributed to the question. After having fled their homes, they now deemed Bessarabia as a fertile soil for the national struggle (King 2000, 31). Besides, already in December 1917, the Romanian forces operated in the region (Skvortsova 2002, 162; cf. Dima 2001, 17).

Moreover, if the unification was apparent, the election of *Șfatul Țării* would have turned unnecessary. Following this interpretation, the reason to establish a cabinet was the need to safeguard the rights of the local élite within a united Romanian Kingdom (Lamminparras 2014a, 46). Thereafter, on January 24, 1918, the *Șfatul* proclaimed Bessarabia's independence, as an alternative to its merger with the Kingdom. In addition, once threatened by Ukraine's territorial ambitions and

ravaged by Bolshevik and other armed units, Bessarabia opted for the union. Despite the presence of Romanian soldiers, the decision yet entailed large regional provisions (King 2000, 33, 35).

The immediate response from the Bolsheviks, with their capital transferred to Moscow, was to interrupt the diplomatic relations with Bucharest and to confiscate the Romanian gold in the Russian banks (Dima 2001, 17). The official historiography of Soviet Russia, later Soviet Union, did not recognize the union. Since the *Sfatul Ţării* failed to represent the whole population, the union of Bessarabia and Romania was illegitimate (Eyal and Smith 1996, 225). This conviction seems to prevail in Moscow, albeit Putin only states in passing "the Romanian occupation of Bessarabia" (Putin 2021). Unlike her President, Zakharova recaps the Soviet years with a column. Her summary is unembellished:

> It wasn't without issues, but together we agonized. Besides that, there were huge achievements (Zakharova-B30O 2024).

Here, Zakharova's descriptive caress weakens, although the spokesperson preserves some of its traits, e.g., the marker 'Besides that'. Instead of active forms of the verbs, Zakharova also moves to utilize the passive ones. This choice, in turn, dispels the subjects, as if Zakharova herself took distance.

Primarily, it remains unknown where Soviet history begins in the eyes of Zakharova. Does she refer to the Moldovan ASSR, founded east of the Dniester within the Ukrainian SSR in 1924 (King 2000, 54, 57; Dima 2001, 22; Yekelchuk 2008, 22)? Zakharova's depiction of the era as "the peak of the development of the scientific, cultural, artistic and intellectual potential of the republic" (Zakharova-B30O 2024) could be read as an allusion to the 1920s–1930s. As outlined in the all-union policy of *korenizatsija* (indigenization), the cultural policy of the MASSR observed the so-called moldovanisation (Yekelchuk 2008, 22). The Central Bessarabian dialect was to provide for the model of the official language, presumably to curtail the separation of the two sides of the Dniester. The first grammar was published in 1925, and the first vocabulary in 1926, but except for the Cyrillic, they were considered too identical with their Romanian equivalents (King 2000, 65). To some extent riotously, the Soviet functionaries themselves were thoroughly aware of the hindrances of the 'Moldovanisation' in 1927. First, the nominal ethnos constituted only one-third of the republic's population, whereas the Ukrainians counted for half. Second, the village culture was a mixture of Moldovan, Ukrainian, Russian, and Jewish traits rather than of indigenous ones. Third, among the cadres in the rural Executive Committees, the knowledge of the Moldovan language was virtually nonexistent (Ţîcu 2019, 207–208).

According to Ţîcu, it was these obstructions that turned the tide. From 1930 on, the Soviet leadership commenced to further the Romanian aspects (Ţîcu 2019, 209). In 1932, the Latin alphabet was introduced (Yekelchuk 2008, 22). Curiously, a new

grammar was produced as late as 1930 (King 2000, 67); it had barely sold before it was brushed aside. Then again, as the all-Union policy in the late 1930s strived to create a wholly new Soviet citizen, stripped of any local attributes, the Cyrillic was reinstated. With the purges of 1937–1938, the old Bessarabian cadres were largely indicted. Instead, the local, Ukrainian, and newly recruited party members took over the Moldovan ASSR (Bruchis 1996, 22; Negru 2003, 54–55, 65). Even here, the analogy is to be found in the Northwest, where the Soviet Union established the Karelian Workers' Commune in 1920, from 1923 to 1940 known as the Karelian Autonomous SSR. Despite the name, it was the Finnish language that prevailed, only to be subjugated in favor of the Karelian idiom. After the Winter War, in March 1940, the KASSR obtained the status of a union republic. Just like in the case of the almost concomitantly founded Moldovan SSR, the solution was to politically signal the benevolence of the Soviet rule, and militarily, to pave the way for a new westward onslaught (Kautto 1989, 31–38).

What is intriguing is that Moscow drives on two tracks while it tackles the 1920s and the 1930s in its southwest. As for Ukraine, Putin sturdily criticizes the early Soviet solutions. According to the Russian president, the nationalities policy led to an artificially demarcated Ukraine (Putin 2021). However, he does not extend his view on Moldova, in his words, "a special case" and "a unique history" (Lamminparras 2024a, 106–108, 112). Putin just briefly states the geographic changes: "in 1940, into the UkSSR were incorporated a part of Bessarabia -- and Northern Bucovina" (Putin 2021). That is, he leaves the door open for diverse interpretations. Analogically, if Zakharova disclosed her actual era of reference, the number of paradoxes would seemingly compromise the narration.

6. Modern(ized) Moldova

Even if Zakharova alluded to the Moldovan SSR, founded in August 1940, the precarious topics would be abundant. After two ultimatums to the Bucharest government, the Soviet army marched into Bucovina and Bessarabia on June 28, 1940 (Dima 2001, 28, 32). The original medieval territory of Bessarabia (today's Southwestern Odesa region), Northern Bucovina, and the county of Herta were incorporated into Ukraine. The remaining 33,700 km² constituted a fresh union republic, the MSSR (King 2000, 95). Zakharova entirely bypasses these phases. On the revulsion of the Axis invasion a mere year later, she leaves no doubt. The spokesperson condemns the recent "whitewashes" in Western Moldova where monuments and a graveyard were constructed "for Romanian soldiers -- who invaded the USSR in the phalanges of Hitler's ally, I. Antonescu". What is even more serious, these memorials were erected not to those "defenders who struggled to save their country, region, and homes from fascism and Nazism" (Zakharova-B13N 2024; Antonescu's dictatorial reign in Romania, Bessarabia, and 'Transnistria' in 1940-1944, see, e.g., Deletant 2006; Ioanid 2023). As such, these allusions serve to undermine Chisinau's reputation, as Zakharova associates them with the Moldovan

rejection to vote for the UN General Assembly resolution on 'The combat against glorification of Nazism', advanced at the time by Russia (Zakharova-B13N 2024).

Apart from the wartime, the administrative reforms, the deportations, the forced collectivization, and the famine of 1946-1947 precipitated the MSSR's Sovietization. Tragically, this eon undeniably unites the Russians and other nations, as stipulated by the Foundations of the State Policy within the sphere of Historical Enlightenment. In the freshly annexed republics, equal measures were conducted to eliminate the traditional social horizon and to lay a basis for a new one. E.g., it is estimated that a total of 33 thousand Estonians were extradited between 1941 and 1951 (Rahi-Tamm 2011, 77, 88). With the notorious March Deportation of 1949 alone, circa 43 thousand Latvians were deported to Siberia (Saleniece 2009, 63). As for Moldova, Zakharova's short notion on the "agonies" (Zakharova-B30O 2024) probably indicates the very same years, sealing the fate of 140 thousand citizens (King 2000, 96; Eyal and Smith 1996, 226). The scale in Bessarabia was particularly severe, since the figure corresponds to roughly six percent of the entire population. Obviously, on this harsh toll it is better to remain silent.

Equally, the history policy was to characterize Moldova as a distinct nation, leading to the censorship of Romanian publications, and to the destruction or desecration of churches and monasteries (the Soviet theories on a so-called Moldovan nation, see Negru E. 2023, 68–72). The demographic changes between 1944 and 1959 diminished the Moldovan majority from three-quarters to two-thirds. Meanwhile, the share of the Russians and Ukrainians together rose from 16 to some 25 percent (Dima 2001, 46, 73–74, 76). Still, while those cadres that originated from Pridnestrovye (east of the Dniester) in the late 1940s pushed to establish a mix of Moldovan, Ukrainian, and Russian as the official language, the old Bessarabian intellectuals successfully resisted the project (Bruchis 1996, 24). Gradually, the scope advanced, and soon the Russian culture reached its hegemony, as it had done a hundred years ago.

However, since the Moldovan SSR persisted as a faraway agrarian republic (Dima 2001, 63), it is most likely that Zakharova implies the 1970s. Particularly, because she describes the Soviet period as "the peak of the industrial and socioeconomical development" as well (Zakharova-B30O 2024). The numbers truly are substantial: whilst Moldova's industrial base in 1970 was rather restricted, between 1971 and 1975 the state-led construction program nearly tripled the amount of small, medium-sized, and heavy production (Dima 2001, 67). As the core of the MSSR's manufacture vastly consisted of the alimentary industry, leading to the republic's heavy dependence on production beyond its boundaries (Ţîcu 2019, 361–362), the large investments certainly augmented Moldova's capacities. Nevertheless, the downsides of the excessive exploitation were erosion of the viticultural soil and an increasing pollution of the rivers (King 2000, 102).

A major impetus to develop the backward republic was the Romanian leader Nicolae Ceaușescu's antipathy toward Moscow since the mid-1960s. The new interpretations in the Romanian historiography, say regarding the annexation of Bessarabia in 1812 and the wartime conduct of the Red Army, fomented a friction between Bucharest and Moscow (Moisa 2015, 129, 131, 133). Thence, the triple aim of the heavy industrialization was to attach the local people to Moldova and to the Moldovan identity, to underscore the country's separateness from Romania, and to generally avert dissatisfaction.

Zakharova virtually lauds this era: during it, "a massive interest was shown in the originality of the Moldovans". At the same time, "the development of the national craft, the professional arts and literature was encouraged" (Zakharova-B30O 2024). However, the measures assumed did not advance these objectives much. Initially, most of the new complexes were erected along the Dniester (King 2000, 99). Naturally, the stream provided for energy. Perchance, the authorities perceived the Eastern bank as more fit, due to its cultural proximity to the Slavs. Especially, the Moldovan language endured an immense russification alongside the industrialization and by the increased distribution of electronics and devices. Likewise, the streets and public premises were renamed after Soviet-Russian heroes (Țîcu 2019, 368). The enormous progress attracted Ukrainians and Russians to settle in the republic, again as it had done a century before. Thus, the regional demography followed the same tendency as during the previous twenty years, although the relative share of the Moldovans and that of the Slavs did not notably alter (King 2000, 97, 100).

Therefore, even this age becomes complicated for Zakharova's assertion. Why did these progresses once more ensue as a reflection of the Romanian policy beyond the Prut? Ironically, the more the Soviet power emphasized Moldova's uniqueness, the more attention was paid to the Romanian heritage (Skvortsova 2002, 175). Urbanization induced Moldovans from the countryside to move to cities; many of these found their place within publication, and subsequently, brought in traditional and national perspectives. As Eyal & Smith conclude, the emerging nationalism and the economic decline notwithstanding, the circumstances in Moldova had by the early 1980s turned flammable (1996, 230). However, as with the latter half of the previous century, Zakharova remains equally tacit on that of the 20th.

Conclusions

If the Moldovan EU-referendum and the concomitant presidential polls in 2024 were a fairytale compiled by the renowned and capable Maria Zakharova, the spokesperson of the Russian MFA, the EU would play the role of the evil Wolf which lures its prey, a unique Moldova. As a striking opposite to the classical tales, the local shepherds are aware of their distinctiveness and their magnificent past with a

third party, the Bear. Thence, they chase the marauder away. Ironically, it is not said that Zakharova could tell such a fable and utilize such metaphors. Instead, neither President Putin nor the Minister of Foreign Affairs Sergey Lavrov has commented on the Moldovan plebiscite. While labelling the Moldovan constitutional reform as a Western intrigue, Zakharova took advantage of repetition and, generally, of a confrontational strategy. Zakharova stresses that the electoral process was thoroughly plagued by the "repression" of individual dissidents and of the independent media. Moreover, the Russian-based Moldovans, aspiring to travel back home to vote, met insurmountable obstacles. As the core Western values and human rights were allegedly violated, the ultimate objective of Zakharova is to defame Moldova and hamper its pro-European integration.

Nonetheless, the electoral conspiracy did not betray the valiant Moldovans living within the borders of the republic. In Zakharova's articulation, these rejected the constitutional reform with an unquestionable majority of some 55 percent. Simultaneously, they expressed "nonconfidence" in President Sandu's government. Chiefly, this is in line with the thesis of Sergeyev on the two convictions that still shape Moldova. Whilst the pro-Romanian leadership promotes Latin origins, it at the same time advocates Western civilization. Conversely, those Moldovans who prefer the Russian language see themselves as a faithful string of the Slavic inheritance, or the Russian world. If one follows Zakharova's utterance, exactly this latter assumption proves the reason for the rejection of the proposed constitutional amendments in favor of the EU. The Moldovans are aware of the membership's ultimate scope, that is, the country would gradually transform into a NATO base. In other words, this is an inexcusable course for a traditionally European nation that cherishes both its "glorious history" and its centuries-old ties with Russia.

Strangely, dodging 1200 years, Zakharova dates the origins of the intense Russo-Moldovan links to the early 18th century. Her assessment – from now on applying a descriptive representation of facts – commences from the Ottoman vassal ruler of Moldavia, Prince Dimitrie Cantemir. The prince is depicted as having advanced the country's "statehood" and its "national identity". As vivid as this illustration is, it omits two essential issues. The Lutsk alliance, largely beneficial for Moldavia, and forged between Cantemir and Peter I in April 1711, collapsed two months later. Thereafter, the cosignatories retreated to Russia. Whilst Cantemir literally enhanced the Moldovan identity of his brethren, he did not make any distinction between the terms 'Moldovan' and 'Romanian'. Paradoxically, as Zakharova underscores the importance of the prince, she in fact refers to the Roman ancestry of the Moldovans – and not to their uniqueness.

The very same inconsistency is inferred in Zakharova's narrative concerning Bessarabia, after it was incorporated into the Russian Empire in 1812. First, the spokesperson is outright descriptive and utilizes many markers, such as "after", "truly", and "from now on". Also, she presents precise figures. Initially, there indeed

manifested some progress and liberalism, as there did in the parallel, the Grand Duchy of Finland. Even so, Zakharova ends her account on educational development in 1860 and the one on economic progress in 1861, with no outspoken grounds. This implies that the latter half of the century may contain precarious precedents. For example, the more freedoms the neighboring principalities of Moldavia and Wallachia obtained, the more the authorities of Bessarabia strived for the region's russification. Russian was made the official language in 1854, and it swiftly overtook the administrative and educational systems of Bessarabia.

The Emancipation Reform in Spring 1861 aggravated the economic situation. In the Southern regions, the surface of arable land available for the freed serfs might have decreased by 40 percent. The poverty drastically increased, and the estimates speak of half of the peasants being unable to sustain their families in 1900. Thence, if Zakharova highlighted the second half of the 19th century as one of the main eras of Moldova's domestic progress, she would have to explain both paradoxes: the economic deterioration and the Russian cultural hegemony.

In the 20th century, the pattern proved identical, except for the union republic – the Moldovan SSR – founded in 1940. Out of the whole period, President Putin laconically states the Romanian "occupation" of Bessarabia in 1918 and the USSR's territorial expansions in 1940. With her allusion to the Soviet era, Zakharova, for her part, most likely refers to the aforesaid union republic rather than to the Moldovan ASSR within Ukraine in 1924–1940. In this latter regard, the Moldovan identity and language were to be codified, but any programmatic development suffered from the all-union policy, which was often steered back and forth. Instead, following Zakharova's description, it was the Moldovan SSR that nurtured a blossom of the native arts, science, and craft. Yet, she avoids revealing how and when, since the Russian language had already in the 1950s gained supremacy in the republic. In contrast to other episodes, Zakharova does denote "the agonies" of the era, that is, the tolls of the Sovietization. However, there is no data or numbers on the losses. As in the case of the Baltic equivalents, these would turn into an ominous precedent. The victims of the Stalinist policy in the MSSR rose to six percent of the population.

Economically, Moldova remained a peripheral agrarian state. To downplay the Romanian leader Ceaușescu's increasing nationalism in the late 1960s, the Soviet leadership initiated a vast industrialization program the following decade. Numerically, its achievements rose to 200 percent. Poignantly, this was the phase that factually enhanced the Moldovan identity, albeit as an unsolicited objective. The more the Soviet authorities construed the distinctiveness of Moldova, the more attraction there occurred in the common Romanian-Moldovan legacy. Just as previously, if Zakharova pronounced a more detailed version on these days, she would encounter identical contradictions as she did with all the previous eons. I.e., the Russian dominance, the likeness of Moldova and Romania, and the financial falloff.

References

Babilunga, N. 2015. *Pridnestrov'ye: shagi istorii* [Pridnestrovie: steps of history]. Tiraspol': MID PMR.

Bărbulescu, M., D. Deletant, K. Hitchins, Ş. Papacostea and P. Teodor. 1998. *Istoria României [History of Romania].* Bucureşti: Editura Enciclopedică.

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.

Bruchis, M. 1996. *The Republic of Moldavia from the collapse of the Soviet Empire to the restoration of the Russian Empire*, translated by Laura Treptow, East European Monographs, New York: CUP.

CCM (Curtea Constituţională a Republicii Moldova, Constitutional Court of the Republic of Moldova). 2024. Hotărâre cu privire la confirmarea rezultatelor alegerilor şi la validarea mandatului de Preşedinte al Republicii Moldova [Decision on confirming of the results of the elections and on validating the mandate of the President of the Republic of Moldova]. November 28, 2024. Chişinău, pdf.

CEC (Comisia Electorală Centrală). 2024a. Rezultatele referendumului republican constitutional [Results of the nationwide constitutional referendum]. Chişinău, pdf.

___. 2024b. Rezultatele alegeri turul I [Election results first round]. Chişinău, pdf.

Deletant, D. 2006. *Hitler's Forgotten Ally: Ion Antonescu and his Regime, Romania 1940-1944*. London: Palgrave MacMillan.

Dima, N. 2001. *Moldova and the Transdnestr Republic*, East European Monographs, No. DLXXIX, New York: CUP.

Dulgheru, V. 2016. *Istoria Integrală a Basarabiei* [The complete history of Bessarabia]. Chişinău: Serebia.

___. 2018. *Istoria Republicii Moldova* [History of the Republic of Moldova]. Chişinău: Tehnica-Info.

Englund, P. 1998. *Pultava: berättelsen om en arméns undergång* [Poltava: Tale of an army's downfall]. Stockholm: Atlantis.

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

Eyal, J. and Gr. Smith, 1996. "Moldova and the Moldovans". *The Nationalities Question in the post-Soviet states*, 223–244, edited by Graham Smith. London: Longman Group.

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

From, P. 2007. *Katastrofen vid Poltava. Karl XII:s ryska fälttåg 1707–1709*. [Catastrophe by Poltava. Carl XII and the Russian campaign in 1707–1709]. Lund: Historiska media.

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.

Ioanid, R. 2023. *La Roumanie et la Shoah – Destruction et survie des Juifs et des Roms sous le régime Antonescu 1940–* [Romania and Shoah – destruction and survival of the Jews and of the Roma under the regime of Antonescu 1940–]. Deuxième édition, traduction Doina Marian, revue Nicolas Weill. Paris: CNRS Éditions.

Jussila, O. 2006a. "Aleksanteri II:n aika [The era of Alexander II]". *Venäjän historia* [History of Russia], 235–260, edited by Heikkinen Kirkinen, Fourth edition. Keuruu: Otava.

___. 2006b. "Nikolai I:n aika [The era of Nicholas I]". *Venäjän historia* [History of Russia], 213–235, edited by Heikki Kirkinen, Fourth edition. Keuruu: Otava.

Kautto, A. (ed.). 1989. *Puna-armeijan marssiopas Suomeen 1939* [The Red Army's march manual into Finland 1939]. Hämeenlinna: Karisto Oy.

King, Ch. 2000. *The Moldovans. Romania, Russia, and the Politics of Culture*. Stanford: Hoover Institution Press.

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».

Kremlin (Prezident Rossii). 2025. Search performed on August 26, 2025.

Lamminparras, N. 2014a. *Mikä on Transnistria? Dnestrin Moldovalaisen tasavallan synty ja nykypäivä*. [What is Transnistria? The birth and today of the Dniester Moldovan Republic]. Master's thesis. Helsinki: University of Helsinki.

___. 2014b. "Vain Venäjän vasalli? Transnistria EU:n ja Euraasian välillä" [Merely a Russian vassal? Transnistria between the EU and Eurasia. *Tiede ja ase* [Science and arms], Vol. 72, Nro 1: 43–74. Helsinki: Finnish Society of Military Sciences. https://journal.fi/ta/article/view/50160.

___. 2024a. "Putin's Implicit War History of the Russians by the Danube in 500-1792". *Revista de Istorie Militară* 3-4:105–114. București: ISPAIM. https://ispaim.mapn.ro/webroot/fileslib/upload/files/RIM/RIM_3-4_2024.pdf.

___. 2024b. "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.

___. 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. Bucharest: "Carol I" National Defence University. DOI: 10.53477/2284-9378-25-14.

Linnarsson, M. 2022. "Sverige och Ukraina under karolinsk tid. Politiska förbindelser och Filip Orliks konstitution 1710 [Sweden and Ukraine in Carl XII's era. Political ties and Philip Orlyk's constitution]". *Karolinska Förbundets Årsbok 2022* [The Annal 2022 of the Carolian Society], 7–17, edited by Magnus Linnarsson. Stockholm, Karolinska Förbundet.

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».

MID-1. (Ministerstvo inostrannykh del Rossiyskoy Federatsii, MFA of the Russian Federation). Search performed on August 26, 2025.

MID-2. Search performed on August 26, 2025.

Moisa, G. 2015. "Chestiunea Basarabiei în imaginarul istoriografic al regimului Nicolae Ceausescu [The Bessarabian question in the historical imagination of Nicolae Ceausescu regime]". *Revista de Istorie a Moldovei* [Review of the Moldovan history] 3(103):129–139. Oradea: Universitatea din Oradea.

Negru, E. 2023. "Elaborarea fundamentelor etnoculturale ale identității naționale din RSMM (1944–1954) [Elaboration of the ethnocultural fundaments ot he national identity of the MSSR (1944–1954)]". *Revista de Istorie a Moldovei* [Review of the Moldovan history] 3-4(135-136): 67–77. Chișinău: USM.

Negru, E. 2003. *Politica etnoculturală în RASSM (1924–1940)* [The ethnocultural policy in the MASSR (1924–1940)]. Chișinău: Prut International.

Negru, Gh. 2023. "Politica țaristă de rusificare a învățământului și „realitățile nefavorabile" din Basarabia (a doua jumătate a sec. al XIX-lea [The Czarist policy of russification of education and „the unfavourable realities" of Bessarabia (the second half of the 19th century)]". *Revista de Istorie a Moldovei* [Review of the Moldovan history] 3-4(135-136): 30–51. Chișinău: USM.

Osnovy. 2024. "Osnovy gosudarstvennoy politiki Rossiyskoy Federatsii v oblasti istoricheskogo proshveshtsheniya". [Foundations of the State Policy of the Russian Federation within the sphere of Historical Enlightenment]. Moskva, pdf.

Putin, Vl. 2021. *Ob istoricheskom yedinstve russkikh i ukraintsev* [On the historical unity of the Russians and the Ukrainians]. Moskva, July 12, 2021. Pdf.

Rahi-Tamm, A. 2011. "Eesti kodanike sundmigratsioon itta aastail 1941–1951: mõningaid võrdlusjooni läände põgenenute looga [Forced migration of Estonian citizens to the East in 1941–1951: on datum lines in the history of refugees to the West]". *Acta Historica Tallinnensia* 17: 72–94. Tallinn: Teaduste Akadeemia Kirjastus.

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

Romanova, Sv. 2022. "Stranitsy istorii: referendum v Gagauzii 02.02.2014 [Pages of history: referendum in Gagauzia 02.02.2014]". *Știință, educație, cultură* [Science, education, culture] vol. 3: 494–498. Comrat: USC.

Roper, St. 2008. "Post-Soviet Moldova's Identity and Foreign Policy". *Europe's Last Frontier? Belarus, Moldova, and Ukraine between Russia and the European Union*, 79–96, edited by Oliver Schmidtke & Serhy Yekelchyk. London: Palgrave Macmillan.

Saleniece, I. 2009. "Läti 20. sajandi ajaloo allikad: suulise ajaloo allikate ja arhiividokumentide dialoog [History of Latvia in the Twentieth Century as Reflected in Historical Sources: Dialogue between Oral History and Archival Records]". *Mäetagused* [The Ultramontane] 43: 61–84, edited by Mare Kõiva, Andres Kuperjanov, Tiiu Jaago and Ene Kõresaar. Tartu: EKM rahvausundi ja meedia töörühm.

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)], [in:] *Kommunikatsija v sovremennom mire* [Communication in contemporary world] 20:115–117. Voronezh: Voronezhkiy gosudarstvenniy universitet.

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

Skortsova, A. 2002. "The Cultural and Social Makeup of Moldova: A Bipolar or Dispersed Society?". *National Integration and Violent Conflict in Post-Soviet Societies. The Cases of Estonia and Moldova*, 159–196, edited by Pål Kolstø. London: Rowman & Littlefield Publishers.

Țîcu, O. 2019. *Homo Moldovanus Sovietic. Teorii și practici de construcție identitară în R(A) SSM (1924–1989)* [Homo Moldovanus Sovietic. Theories and practices of identity construction in M(A)SSR (1924–1989)]. Ediția a doua. Chișinău: Editura Arc.

Yekelchyk, S. 2008. "Out of Russia's Long Shadow: The Making of Modern Ukraine, Belarus, and Moldova". *Europe's Last Frontier? Belarus, Moldova, and Ukraine between Russia and the European Union*, 9–29, edited by Oliver Schmidtke & Serhy Yekelchyk. London: Palgrave Macmillan.

Zakharova-K21O. 2024. Kommentariy ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy po itogam pervogo tura prezidentskikh vyborov i konstitutsionnogo referenduma v Moldavii [Commentary of the official representative of the Russian MFA, Maria Zakharova, on the results of the first round of the presidential elections and on the constitutional referendum in Moldova]. Moskva. https://mid.ru/ru/foreign_policy/news/1976983/.

Zakharova-B23O. 2024. Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy, Moskva [Briefing of the official representative of the Russian MFA, Maria Zakharova, Moscow]. https://mid.ru/ru/foreign_policy/news/1977268.

Zakharova-B30O. 2024. Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy, Moskva [Briefing of the official representative of the Russian MFA, Maria Zakharova, Moscow]. https://mid.ru/ru/foreign_policy/news/1978331/.

Zakharova-K04N. 2024. Kommentariy ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy o vtorom ture prezidentskikh vyborov v Moldavii [Commentary of the official representative of the Russian MFA, Maria Zakharova, on the second round of the presidential elections in Moldova]. Moskva. https://mid.ru/ru/foreign_policy/news/1979108/.

Zakharova-O07N. 2024. Otvet ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy na voproz CMI o stituatsii v Moldavii [Reply of the official representative of the Russian MFA, Maria Zakharova, to questions of the media on the situation in Moldova]. Moskva. https://mid.ru/ru/foreign_policy/news/1979818/.

Zakharova-B13N. Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy, Moskva [Briefing of the official representative of the Russian MFA, Maria Zakharova, Moscow]. https://mid.ru/ru/foreign_policy/news/1981488.

Zakharova-B21N. 2024. Brifing ofitsial'nogo predstavitelya MID Rossii M.B. Zakharovoy, Moskva [Briefing of the official representative of the Russian MFA, Maria Zakharova, Moscow]. https://mid.ru/ru/foreign_policy/news/1982671.

ACKNOWLEDGEMENTS

I express my profound gratitude to my late foster brother Taneli, who departed on May 7, 2025, for the enjoyment and the young perspective he brought to my daily life and research work.

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 on the sites of the Kremlin and the Russian MFA (in Russian).

DECLARATION on AI use (if applicable)

N/A

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Adaptive Military Leadership in the Digital Age

Assistant Professor, Abdulkadir AKTURAN*
Professor, Mustafa Taner ALBAYRAK**
Professor, Aykut ARSLAN***

*Faculty of Economics and Administrative Sciences, Piri Reis University/Turkiye
e-mail: aakturan@pirireis.edu.tr
https://orcid.org/0009-0008-9107-0333
**Faculty of Economics and Administrative Sciences, Piri Reis University/Turkiye
e-mail: talbayrak@pirireis.edu.tr
https://orcid.org/0000-0002-4743-9235
***Faculty of Economics and Administrative Sciences, Piri Reis University/Turkiye
e-mail: aarslan@pirireis.edu.tr
https://orcid.org/0000-0001-5689-3918

Abstract

The digital age has dramatically transformed the face of warfare, disrupting conventional military paradigms. Leaders require cognitive agility, digital fluency, and moral resilience to successfully navigate these new military paradigms. In this paper, we examine the promising new form of adaptive military leadership in the rising convergence of artificial intelligence, cyber conflict, autonomous systems, and multi-domain operations. Using an assessment as well as the Russia–Ukraine war and NATO strategic recalibrations as a case study to generalize critical capabilities and institutional transformations necessary for effective military leadership in the 21st century, this article will explore realizable avenues. The adaptive leadership framework draws on the way leaders sense adaptive challenges, regulate distress levels in times of change, and focus attention. Based on these, the study will analyze how military organizations develop leaders who are not only technologically good but also ethically sound and make good judgments in ambiguous and changing situations. This paper will explore digital ethics, systems thinking, and cross-domain operations in professional military education. It argues that creating interdisciplinary learning, fostering experimental environments, and forming steps to build future commanders able to thrive in the chaos and help shape the future of warfare are absolutely necessary steps. Finally, this article will demonstrate that such agile, technologically literate, and ethically grounded leaders need to be developed for achieving operational effectiveness in a highly complex and uncertain modern battlespace with great levels of dynamism.

Keywords:
Military Leadership; Adaptive Leadership; Digital Warfare; Cognitive Agility; Hybrid Conflict; Strategic Command; Defense Transformation.

Article info
Received: 7 July 2025; Revised: 5 August 2025; Accepted: 2 September 2025; Available online: 6 October 2025

Citation: Akturan, A., M.T. Albayrak and A. Arslan. 2025. "Adaptive Military Leadership in the Digital Age." *Bulletin of "Carol I" National Defence University*, 14(3): 29-58. https://doi.org/10.53477/2284-9378-25-35

Introduction

The nature of warfare has evolved beyond the very tangible realms of armored vehicles and dug-in fighting positions (Kott, Alberts, and Wang 2015). The battlefields of tomorrow are taking shape today in the highly complex domains of cyberspace, satellite constellations, and code-speaking a language so advanced. In such a quickly changing environment, conventional forms of military leadership fit ever less. As NATO put it in its 2022 Strategic Concept, the defining characteristics for security in this 21st century are 'technological innovation and strategic competition.' The question that now stands before modern defense establishments is no longer whether they should change but how fast they can effectively transform into something else.

The article discusses the essential requirements for an adaptive military leadership approach in the new digital age, an approach that not only survives the challenging landscape but thrives in it. It therefore forms a reinterpretation of Heifetz's Adaptive Leadership Framework within military command, further elaborating important functions in this specific context, such as identifying adaptive challenges, regulating distress, and maintaining disciplined attention. Leadership is viewed as the agile practice of mobilizing people to take on and solve large problems while building resilience and achieving success in conditions of uncertainty, complexity, and conflict (Deep 2023). Applying this framework to modern defense organizations will show how its fundamental principles unfold into cognitive, ethical, and digital competencies required by future battle environments. Leaders need to build adaptive decision-making skills as artificial intelligence and autonomous systems gain more space. This exploration considers the reforms needed for building adaptive leaders by instituting digital ethics, systems thinking, and cross-domain operations into military education.

Methodology

The study applies a qualitative case study to trace the evolution and implementation of adaptive military leadership in the digital age. A triangulated analysis of doctrinal reviews, real-world military engagements, and leadership theory serves to develop an integrative understanding of how modern military institutions might evolve to better cultivate leadership capabilities in technologically saturated and ethically ambiguous environments. Data sources included:

- Doctrinal documents such as the 2022 Strategic Concept of NATO and U.S. Joint All-Domain Command and Control updates (Navaratna 2025);
- Case studies of recent conflicts: the Russia–Ukraine war, the 2020 Nagorno-Karabakh War, and the Israel–Iran hybrid conflict, processed through scholarly and institutional reports (Kahn 2022; Khalilzada 2024; Baram and Ben-Israel 2025);
- Adaptive leadership frameworks by Heifetz and others (Heifetz, Grashow, and Linsky 2009; Boikanyo 2025).

AI and autonomous systems literature on military application, command ethics, and leadership implications (Bankins, et al. 2024; Matli 2024; Taddeo, et al. 2022). These works were combined in an interpretive framework of themes that sought core competencies, cognitive agility, digital literacy, and moral resilience, plus institutional imperatives like decentralized command, ethical integration of AI, and a leadership development model. Thus, patterns, differences, and actionable insights spanning national and organizational borders were noted through cross-case comparison. In this way, leadership imperatives could be inductively formulated from the realities of practice, supported by theoretical logic aimed at reforming military education.

1. Technology and the Transformation of Warfare

1.1. Beyond Kinetics: The Rise of Digital Battlespaces

Modern warfare has fast transitioned into non-kinetic domains, from the electromagnetic spectrum to the cognitive domain. Over 70% of success in recent simulations is based on effective digital situational awareness and real-time data fusion, as highlighted in the update for 2024 Joint All-Domain Command and Control by the U.S. Department of Defense (Navaratna 2025). This concurs with NATO Strategic Concept 2022: Technological innovation and strategic competition are defining features of the security landscape of the twenty-first century. At the Vilnius Summit held in 2023, it was once reaffirmed that digital capabilities, artificial intelligence, machine learning, and cyber defense are critical to defense modernization (Achuthan, et al. 2024). An excellent example of how these trends play out in practice is the performance of Ukraine's military during the ongoing conflict with Russia. Even with asymmetries in manpower and equipment, it appears that Ukraine has been successful in leveraging commercial satellite communications, social media for strategic messaging, open-source intelligence, and rapid decentralization of decisions at the battlefield level (Kahn 2022; Kushnir and Chernobai 2020). This will involve not only achieving better tactical outcomes but also winning international public opinion (Kot, et al. 2024). Therefore, effective digital technology assimilation demands equally effective leaders who can make decisions in such rich-data, rapidly changing environments.

The conduct shows the edge of adaptive, innovative management housed in a structure that is digitally uplifted. In reality, the Israeli Unit 8200 offers evidence in support of hard technologies with real-time cognitive mapping of the landscape, fusing sensor input with social media interpretation to monitor hybrid threats within the complex Israel-Iran conflict (Pahlavi and Ouellet 2012). By 2024, at least 60 nations will have some version of loitering munition or combat drone technology available to them, an increased trend towards autonomous systems (Baccino, et al. 2025; Hozint.com 2025). These underscore requirements for military leaders to be tech-savvy and able to weave varied digital implements into total strategies that change as circumstances shift quickly. The multi-domain operations that mean the fusion of capabilities across land, air, sea, space, and cyberspace require leaders

who can delegate authority in decentralized structures. They should also be able to synthesize sometimes even contradictory streams of complex information to enable strategic clarity under uncertainty. Such adaptive decision-making skills must also be possessed by commanders to assess critically the directives generated by AI because it is a fallible tool subject to error, bias, and manipulation (Clark, Patt, and Walton 2021). Thus, AI literacy, algorithmic responsibility, and the ethics of digital warfare are being integrated into officer education pipelines in training programs throughout NATO and allied forces (Chen, et al. 2024).

1.2. Autonomous Systems and AI Command Support

The autonomous systems have essentially made the jump from being mere experimental tools to becoming critical operational assets. This quick transition has drastically changed the face of modern warfare. By 2024, more than 60 nations had had some form of combat or loitering drone capability (Ardiansyah 2025). These facts also reflect that the market for military AI systems worldwide is projected to grow up to $18.8 billion by 2027 (Horowitz 2019). For example, Turkey's AI-integrated KARGU-2 are drones that could autonomously find their targets, and Project Convergence 2024 of the U.S. Army, which aims at semi-autonomous coordination between air and ground robotic units (Pretto, et al. 2020; Edmonds, et al. 2021).

The proliferation of such systems also raises enormous ethical and strategic dilemmas. Risks associated with a system that heavily relies on opaque decision models of AI were underlined in the 2023 Geneva Dialogue on Autonomous Weapons, which, above all, stressed the necessity of human-in-the-loop control, especially for lethal systems (Achuthan, et al. 2024; Tamburrini 2021). The challenges in accountability due to opacity in AI have led to yet another consideration: algorithmic bias and unintended consequences (Dhopte and Bagde 2023). Commanders, therefore, need adaptive decision skills to critically assess, audit, or even override AI-generated directives, bearing in mind that while powerful, AI is fallible to error, bias, or manipulation—all the more critical within complex dynamic battlefield settings where unforeseen circumstances can rapidly render pre-programmed algorithms obsolete, even detrimental.

The use of AI in military command structures also calls for a change in leadership paradigms. Leaders should perceive AI not merely as a tool but as an agent constituting complexity within a larger scheme (Simpson, et al. 2021). This means knowledge about limitations of AI, its possible vulnerabilities to adversarial attacks, and its influence on human decision-making. Therefore, training programs at NATO and allied forces are now embedding AI literacy, algorithmic responsibility, and ethics of digital warfare into the officer education pipelines to fulfill these requirements (Porkoláb 2020; Taddeo, et al. 2022). This education will make officers view critically the capabilities and limitations of AI and ensure that its use is responsible and ethical in military operations.

Beyond ethics, this integration produces strategic challenges because now, with more and more use of AI, there might be fresh vulnerabilities to cyberattacks and electronic warfare that can conditionally disable command and control systems and thus frustrate strategic objectives. Adaptive leaders must be skilled in forecasting such risks as well as in creating resilience against technological disruption (Hagos and Rawat 2022). They must also balance the benefits that come with the use of AI with maintaining human control and keeping autonomous systems to uphold strategic goals consistent with ethical principles.

2. Characteristics of the Adaptive Military Leader

The military leader of today should represent a mixture of technical understanding, ethical values, and strategic thinking. They will have to command not only the forces but also manage the integrated digital environments. Adaptive Leadership is a model of leadership that allows the person and the organization to lead in complex, dynamically changing settings. Adaptive leadership theory was founded based on the teachings of Ronald Heifetz at Harvard University and developed in the 1990s because traditional leadership models were inadequate to provide solutions for challenges that involved learning, innovation, and change. In his early work, Heifetz concentrated on leadership within political and organizational domains; however, he primarily articulated the differentiation between technical problems that can be addressed through existing knowledge and procedures and adaptive challenges necessitating experimentation, discoveries, and adjustments of values. According to Heifetz, the work of adaptive leaders involves us in three primary functions: identification of adaptive challenges, regulation of distress, and sustaining disciplined attention (Nikolaou, et al. 2007). These functions offer a guide for leaders who want to successfully maneuver through complex and unclear situations. Ronald Heifetz originally formulated this theory in the 1990s, and since then, it has evolved into a strong framework for leading amid uncertainties, changes, and systemic disruptions (Boikanyo 2025; Heifetz, et al. 2009). Adaptive Leadership was first introduced by Ronald Heifetz in his seminal book, Leadership Without Easy Answers (1994), later with co-author Marty Linsky in Leadership on the Line (2002), and with Alexander Grashow in The Practice of Adaptive Leadership (Heifetz, Grashow, and Linsky 2009). These three works spring from his work at Harvard Kennedy School, where he tried to redefine leadership as a process, not a position. Drawing extensively on systems theory, political science, and psychodynamic theory (Heifetz, Grashow, and Linsky 2009), it highlights the need to make a clear distinction between problems that can be dealt with using available knowledge and processes (technical problems) and those that cannot and hence require new learning, innovation, and value-oriented behavioral adjustments (adaptive challenges). The theory emphasizes the importance of distinguishing between technical problems, which can be solved with existing knowledge and processes, and adaptive challenges, which require new learning, innovation, and adjustments in values and behaviors (Bailey, et al. 2012).
For leaders to flourish in such conditions, they need to possess a set of crucial traits

and hence create organizational cultures that embrace innovation, flexibility, and openness (Sott and Bender 2025). Heifetz makes a distinction between technical problems that can be addressed with the knowledge and procedures already available and adaptive challenges that require innovation, learning, and even changes in values and beliefs or behavior. Therefore, "Adaptive Leadership" can be defined as "the practice of mobilizing people to tackle tough challenges and thrive" (Heifetz, Grashow, and Linsky 2009, 14). The rapid adaptation of strategies and tactics based on real-time data and evolving threats is a capability that leaders must have (Matli 2024). To harness the potential of AI effectively, leaders must develop an organizational culture that encourages both exploration and exploitation (Bankins, et al. 2024). This means promoting experimentation for new applications of AI as well as implementing validated AI applications to enhance productivity and quality of decision-making (Bankins, et al. 2024). In addition, military leaders should have the capacity to evaluate the ethical impacts of using AI (Nalin and Tripodi 2023).

A military leader of this era must possess, in addition to traditional requirements of technical, ethical, and strategic education, the ability to command not only forces but also integrated digital ecosystems. In short, the new military leader should be a hybrid thinker: possessing intimate knowledge of human and machine capabilities alike. They value openness, justice, and accountability for AI systems while addressing biases and ensuring data privacy. The primary responsibility involved in developing AI systems is to build a moral framework within which such systems would operate based on several fundamental ethical principles: justice, transparency, accountability, and human welfare. These individuals are deeply familiar with the capabilities and limitations of AI, understanding how algorithms can augment — but never replace — human judgment. Further, adaptive leaders need to display a high degree of cultural sensitivity awareness, especially in multinational operations. The adaptive leadership approach has been highlighted in studies concerning military and organizational dynamics as a way to deal effectively with complex and imprecise issues (Boikanyo 2025). In military leadership, these functions correspond to some specific abilities:

Cognitive agility: It involves not just apprehending new threats but rapidly assessing such elaborate circumstances so as to be able to foresee further challenges and revise strategies accordingly (Good 2014). It implies a way of thinking that welcomes change and is ready to forsake old assumptions. In other words, cognitive agility at work means the ability of leaders to switch quickly between different styles of thinking, analytical, and intuitive, and to combine varying pieces of information for making decisions (Johnco, Wuthrich, and Rapee 2013). The present war in Ukraine is an illustration of this requirement, as the commanders have had little time in which to adjust to novel technologies and methodologies of warfare.

Digital Literacy: Military leaders of today must have intimate knowledge of digital technologies and their strategic implications, besides being able to use them effectively (Antoniuk and Zasiadivko 2023). They should be able to evaluate the risks

and opportunities of new technologies that come into the military domain with all their possible applications (Türk 2023). Digital literacy is also defined as knowledge about the principles that rule cyberspace, including cyber warfare and information operations through social media for strategic messaging. It was illustrated in the Azerbaijan-Armenia clash where drone warfare with on-the-spot monitoring gave one side strategic superiority (Wu 2022).

Moral Compass: This entails making military leaders grounded in robust moral compasses because the integration of autonomous systems and AI brings to the fore significant ethical dilemmas. This means deepening the understanding of ethical principles and how they apply to complex and ambiguous situations (Uddin 2023). It also means making them promoters as a function of their leadership role of ethical behavioral culture within the military in general and specifically ensuring that all personnel are very aware of their responsibilities per international law and the laws of armed conflict (Crayne 2025; Zanglin 2017). Therefore, investment in ethical AI training is necessary to develop commanders who can handle such dilemmas.

Inspiring Leadership: Adaptive leaders share more of their authority with subordinates. They instill in them the confidence to make decisions at different levels of decentralized decision-making, trusting that the subordinates will take appropriate actions. This, therefore, entails belief in the abilities of subordinates and a readiness to embrace risk and tolerate mistakes (Huettermann, et al. 2024). In addition to delegating authority, they also ensure that resources are made available to support the success of subordinates and thereby foster an accountability culture and continuous improvement (Dias 2024). This competency has been demonstrated by Ukraine's very fast decentralization of decisions on the battlefield.

Cultural and strategic understanding: Contemporary military operations necessarily include interaction with diverse populations and multilateral partners, so cultural sensitivity and awareness must be high among leaders. That is to say, the understanding of different people's cultural norms, values, and beliefs, as well as effective cross-cultural communication (Herrero and Suengkamolpisut 2005). Adaptive leaders should also understand the strategic implications of their actions and decisions on relationships with allies and partners. Leadership in such an intense environment has to be particularly ethical (Robinson, McKenna, and Rooney 2022). In addition, military leaders are required to have excellent knowledge of the cultural, social, and political milieus (Sriharan, et al. 2022). This pertains to the knowledge of media influence, perception, and world norms over military operations. Such awareness also entails the skillful capacity to communicate with different publics and to establish relationships with key stakeholders (Moreno 2021). The Israeli military leadership shows agility by coordinating in real-time across multiple agencies, which is a demonstration of strong strategic awareness.

These skills are linked and build on one another. Developing them means taking a whole approach to military teaching and training, one that focuses on critical thinking, problem-solving, and good thinking about right and wrong (Jnitova, et al. 2021). By building these traits in their leaders, military groups can improve the way they adjust to new situations, encourage new ideas, and get good results in a more complex and unclear world. This framework enables leaders to separate the two: technical problems, which can be solved by using current know-how; and adaptive challenges, which require learning, innovation, and a culture shift. Most challenges in modern warfare fall into the second category. The distinction is critical because treating adaptive challenges as technical problems leads to misapplication of resources and approaches, and hence frustration and resistance, resulting in failure to address the issues (Pak, et al. 2020). Since Heifetz first thought of it, adaptive leadership has been taken up more and applied in many areas, like education and health care, as well as the military (Boikanyo 2025). Adaptive leadership has been prescribed for the military to lead effectively amidst changing threats and technology (Papersowl.com 2023). The fast-changing environment of modern asymmetric conflict and cyber warfare, plus the rise of autonomous systems, requires leaders who can change with the times and help their organizations be more creative.

The stress on ethical grounding shows the weight of moral reasoning and ethical decision-making in the time of self-reliant weapons and data-led war (Askew 2023). Leaders have to be ready to steer through complex ethical dilemmas and make sure that tech advances line up with ethical rules and strategic goals. Adaptive leadership helps us understand the challenges of modern warfare. It can help military leaders develop cognitive agility, digital literacy, ethical grounding, delegative authority, and cultural as well as strategic awareness to enhance their ability to adjust to changing circumstances, innovation, and decision-making ethics (Ertürk and Albayrak 2020). With this in view, as military organizations continue to face complex challenges in the security environment of the 21st century, they must increasingly apply the principles of adaptive leadership for successful operations.

3. Adaptive Leadership in Contemporary Conflicts: Case Studies

3.1. Russia–Ukraine War

The military performance of Ukraine in the conflict with Russia underscores adaptive leadership in war today. There were great asymmetries between manpower and equipment, but innovative strategies allowed for remarkable resilience and effectiveness (Sanders 2023). A major enabler of this adaptability has been the effective exploitation of commercial satellite communications, "Starlink", to maintain connectivity and coordination when under attack from Russian cyber and electronic warfare (Daly 2025). In the words of a report by The Royal United Services Institute, Starlink has provided a lifeline advantage to Ukrainian forces with unbroken

communications, better gathering of intelligence, and improved command and control capabilities (Watling and Reynolds 2022). Besides this, Ukraine waged info ops through social media for message discipline. This was described as domestic and international audience communication that garnered Ukraine support, beat back Russian propaganda, and framed the narrative on the conflict (Mejova, et al. 2023). Social media is proven by academics to be a powerful tool that can shape public opinion and tilt the course of conflicts. Ukraine's use of social media is outstanding in terms of how well it has excelled in recruiting volunteers, fundraising, and organizing humanitarian aid.

Open source intelligence has consequently become a key factor in Ukraine's adaptive style of conflict leveraging. It easily makes use of readily available information from social media, satellite images, and other sources to glean insights on the movement, logistics, and intentions of Russian troops (Zakharchenko 2025). OSINT has enabled Ukraine to make educated guesses about what the Russians will do next and, hence, deploy resources more effectively (Kudlenko 2023). In such a trend, the study of the Atlantic Council also emphasizes how much open-source intelligence is gaining access to modern warfare with its potential of leveling the playing field between adversaries (Harper and Cross 2024). In addition, rapid decentralization by Ukraine of decisions related to the battlefield has given sufficient authority at the lower levels to commanders to act upon changing circumstances and avail themselves of opportunities as they present themselves. Decentralized command has allowed Ukrainian forces to adjust to the fluid nature of the conflict and preserve operational flexibility.

Russian rigid hierarchies and old-fashioned doctrines have blocked command flexibility, against which Russian forces find it much more difficult to adjust to an ever-changing battlefield (Dickinson 2022). It is, therefore, less adaptable because of the rigid organization of the Russian military and old doctrines (Caro 2025). Scholarly accounts attribute the failure of the Russian forces to match Ukrainian tactics to a top-heavy command structure and an apparent absence of initiative on the part of subordinate levels (Faro 2024). Such inflexibility eventually led to tactical defeats and strategic mistakes. Whilst the Russian armed forces have had specific strengths, for instance, in areas of technological advancement and mass operations, their rigid hierarchies and adherence to traditional doctrines have done much to limit flexibility (Caro 2025). Scholarly research, including highlighting the top-down command framework and lack of initiative at lower levels, suggests that these have done much to encroach upon their ability to perform effectively in the context of shifting battlefield dynamics (Faro 2024). This rigidity has resulted in operational delays and strategic miscalculations. Furthermore, influence campaigns have not been able to overcome deep-seated beliefs and negative perceptions (Demus, Holynska, and Marcinek 2023).

The rigid top-down command hierarchy of the Russian military suppresses rapid decision-making (Teixeira, et al. 2024). The hierarchy tends to suffocate initiative

among lower levels, excluding the ability of ground commanders to respond quickly to evolving circumstances. The tightly held adherence of the Russian military to outdated doctrines has proven problematic within the dynamic and fluid nature of war in the contemporary era (Caro 2025). The war in Ukraine has put to the test the weakness of such doctrines in the face of an adaptive Ukrainian strategy. Despite the advances that have been made in military technologies, the Russian military has struggled to incorporate such technologies into its command and control. This has hindered their ability to make the fullest use of digital instruments and information warfare (Mikayılov and Bayramov 2019). Innovation is also stifled as a lack of adequate encouragement of thinking and problem-solving at lower levels does not allow adaptive solutions to unexpected challenges. Tactical and strategic mistakes that turn into operational failures come from the same place: lack of adaptability. The different arms of the military are suffering from poor communication and coordination between them. This has made them unable to effectively counter Ukrainian tactics. Influence operations have so far failed to either shift public opinion or break the resolve of Ukrainians; this speaks to a deficit in understanding of the information environment as well as an inability to adapt messaging strategies (Demus, Holynska, and Marcinek 2023).

3.2. Azerbaijan–Armenia Clashes (2020 Nagorno-Karabakh War)

The 2020 Nagorno-Karabakh War is an excellent example of how adaptive leadership combined with technological superiority can change the rules of engagement in war (Iskandarov and Gawliczek 2021). Azerbaijan won not just by having a better military but through strategic and tactical flexibility in using emerging technologies (Koukoudakis 2024). Importantly, in the context of this study, it was the ability to operationalize Turkish-manufactured Bayraktar TB2 drones that delivered real-time intelligence, surveillance, and reconnaissance (ISR) capabilities and targeted precision strikes against specific Armenian military targets. These drone attacks proved pivotal in limiting 292 disruptions to adversary infrastructure and materially affecting its combat capabilities. It is important to note, however, that drone attack video recordings were also electronically communicated via social media and other digital outlets, resulting in psychological effects, influencing international perceptions, and bolstering Azerbaijan's advantages on the battlefield and in the information warfare domain (Crowley 2025).

Academic conflict analysis pivots on key dynamics. One is offered by Svante Cornell (2017), noting that Azerbaijan has actually achieved significant modern military technological—not strictly weaponry but rather drone technology—operational superiority. Continuous surveillance and strike capabilities open for Azerbaijan to bypass the Armenian defensive measures. Broader strategic adaptation entailed integrating drone warfare with conventional land forces through campaign outcomes. Analysis shows how information dominance for Azerbaijan means to combine military and media operations to shape narrative dominance of a conflict, as well as lower enemy morale; drone footage shared on

social media had extraordinary psychological effects, inflating perceptions over Azerbaijani dominance (Khalilzada 2024). Azerbaijan used it well for projecting its military success on social media, lowering Armenian morale. The command-and-control perspective indicated dynamic command structures within which the Azerbaijani dispersed units operate. Such agility, whereby vulnerabilities are discovered, results in momentum being kept throughout the conflict. The Armenian forces, however, were less adaptive and constrained by old doctrines. It significantly hindered their responsiveness by failing to apply new technologies to operations (Cheterian 2022). Therefore, this war is another evidence of the growing importance of adaptive leadership in a contemporary digital world where rapid technological transformations define the evolution of warfare (Raska 2019).

Furthermore, the utilization of real-time surveillance with drone and satellite images provided Azerbaijan with the most effective knowledge of the operating environment. This facilitated sound decisions and rapid responses to any emerging threats. Its precision-strike capability allowed it to strike necessary military and infrastructure assets with minimal collateral damage. A working, networked communications setup allowed for working and unblocked coordination between different units tied to a shared operating picture and fast information spread (Pashayeva 2023; Sobb, Turnbull, and Moustafa 2023). The Azerbaijani case shows how adaptive leadership, when mixed with technology, can lead to gaining a huge strategic edge. By giving local commanders agency to make decisions based on situational awareness, Azerbaijani forces could maintain flexibility and identified tactical opportunities as they presented themselves (Bankins, et al. 2024). It is important to emphasize that adaptive leadership was more than just using new capabilities, but instead reconfigured the way the military organization operated and made decisions. The successful integration of autonomous platforms with electronic warfare capabilities gave Azerbaijan a significant strategic advantage. These capabilities enabled the disruption of Armenian communications and mitigated air defense systems.

The Armenian military did not prove very apt in adaptive military leadership. They were facing an opponent with better technology, yet the Armenian command structure continued to be hierarchical and reactive. That meant there was little room for operational flexibility and responding on the battlefield. A rigid system like that described by Koukoudakis (2024) makes the forces unlikely to respond effectively to drone warfare against them, and when intelligence and targeting functions are integrated in real time against them. The Armenians fell back on traditional concepts of defense due to no experience with new technologies available to provide such things as AI-enabled surveillance or automated targeting systems; thus, that further reduced their capacity for adaptability at the operational level (Feldman, Dant and Massey 2019). Adaptive leadership is also about controlling information operations and civil-military communication. In this respect, Azerbaijan's perception management through controlled media certainly trumped Armenia's strategic communications, which brought public morale down considerably and international

support even lower (Chernobrov 2025). Finally, adaptive leadership means having emotional resilience and the ability to build cohesion under stress. Armenia struggled to maintain troop morale and organizational unity amid asymmetric threats, suggesting further adaptive capacity deficits. While some localized adaptive actions may have occurred, the broader strategic posture of the Armenian military revealed a lack of preparation for high-tech, hybrid warfare scenarios (Frappi 2023). Scholarly assessments thus stress the necessity of systemic reforms, including the development of decentralized leadership cultures, the incorporation of technological literacy into officer education, and the institutionalization of adaptive leadership principles to strengthen operational resilience and strategic flexibility.

The 2020 Nagorno-Karabakh War is an exemplary turning point in modern warfare. By Azerbaijan, the employment of drone warfare and real-time surveillance with Turkish–Israeli technological platforms (Koukoudakis 2024) have aptly demonstrated how adaptive leadership can decisively shape battlefield outcomes. Strategic dominance was secured for the Azerbaijani Bayraktar TB2 by media campaigns and electronic warfare, as well as autonomous systems synergized by the commanders (Rustamzade and Valiyev 2024). Exploiting rapid technological asymmetries at a pace typical in adaptive leadership theory collapsed further command through dispersed units (Crivellaro 2013; Mikayılov and Bayramov 2019). The main elements that have determined success for military operations are the factors that define how well a state can achieve technological asymmetry, decentralized unit coordination, and general information space management.

3.3. Israel–Iran Hybrid Conflict

The confrontation between Israel and Iran represents a paradigmatic example of hybrid warfare, where cyberattacks, precision strikes, proxy operations, and disinformation campaigns are deployed in conjunction. Although not a conventional war, this conflict illustrates how adaptive leadership manifests through divergent approaches on both sides (Beretas 2020). Israel and Iran have each demonstrated adaptability in ways tailored to their strategic goals, resources, and operational philosophies.

A major enabler of Israel's adaptability has been the high-level integration of cyber and intelligence technologies. Israel has leveraged its superiority in cyber capabilities to carry out both defensive and offensive operations, including cyber espionage, infrastructure protection, and cyber sabotage (Baram and Ben-Israel 2025). The pre-emptive doctrine of Israel is based on the National Security Strategy Principle, which emphasizes rapid response to perceived threats, therefore allowing swift military decisions, normally in the offensive mode. Apparently, in the future, up to 2025, covert operations, precision assassinations included, will remain as a tactical feature within that doctrine, reflecting commitments to technological sophistication with less collateral damage. Apart from that, success has been reflected with Israel in multi-agency coordination whereby military and intelligence together with civilian cyber agencies work towards real-time threat identification, cross-sector collaboration, and synchronization of

operational response supported by interagency agreements plus routine joint exercises (Nyemann and Sørensen 2019; Tabansky 2020). This is ensured through structures that allow for a fluid and dynamic adaptive response to a hybrid threat.

Iran adopted a variant model of the adaptive leadership concept within the asymmetric warfare paradigm. Iran has developed decentralized proxy forces, such as Hezbollah and Hamas, among others, who predominantly operate from their bases but share an ideological alignment within Iran's strategic objectives (Congressional Research Service 2021). Decentralized command manifests itself in allowing for localized decision-making and sustaining processes of implementing activities. The center pillar also guns up cyber warfare capability in its strategic arsenals. Infrastructure attacks against Israeli installations and disinformation campaigns to destabilize Israeli society while polarizing it are now conducted increasingly competently (Arasli 2007; Meriläinen 2025). Digital influence operations—that is, fake accounts and coordinated propaganda campaigns—have extended further wings to operational reach into actual psychological areas. Iran places primary emphasis on leveraging flexible low-cost high-impact tactics – for instance, small boat naval maneuvers as well as mine warfare, including cyber infiltration – revealing adaptive doctrine innovation derived even under resource constraints (Saikal and Vestenskov 2020). Open-source intelligence has been at play on both sides. For example, Israel employs big data analytics and social media monitoring to track proxy movements as well as the shifts in narratives, and then fuses such insights into real-time decisions (Hoffman, Neumeyer, and Jensen 2024). Iran, via proxies and non-state actors, uses the same digital channels to shape public discourse and perception in the information environment.

This hybrid environment thus highlights the complexity of modern military involvement with blurred lines between war and peace. Wu (2022) notes that prior to, during, and after the kinetic operation, critical infrastructure is paralyzed by acts in cyberspace sowing confusion. Clarke (2024) describes information operations—disinformation and propaganda— targeting morale of the population and the public presumption of unattributed sources seemingly tidily. The playing field further widens with moral ambiguity when unconventional international law non-state actors are drawn in (Raugh 2016). Constant readjustment comes into play in this hybrid warfare; this is established based on empirical evidence whereby the Iranians and Israelis adapt their tactics dynamically on all emerging fields, be they cyber intrusions or shifts in political landscapes (Hwang and Joo 2023). In line with such rapid technological advancements as AI-enabled targeting as well as autonomous drone platforms, a shift in paradigm within military leadership culture decision-making is equally demanded (Weidman 2021).

The value of resilience in such a conflict is paramount. Both nations have undertaken steps toward infrastructure hardening, enhancing the survivability of critical assets like power grids, communications networks, and command-and-control systems

(Roshanaei 2021). Cybersecurity practices—including encryption, real-time threat monitoring, and cyber hygiene education—are central to resilience in the digital battlespace (Thakur and Pathan 2020). Mitigating high morale, remaining united as a team, and showing good leadership, particularly under stress, must be part of lasting through sustained and ambiguous fight times (Beckner, et.al. 2021; Smith 2024). In both scenarios, speed and agility as adaptive leadership were seen as imperative. Leaders need to scan changing dangers, lead cross-functional teams, talk openly, and allow new thinking when unsure (Sott and Bender 2025). While Israel does well at putting top tech tools together with real-time working as one, Iran has used the spread of power to help flexible proxies who can carry out changing plans in the field.

The Israel-Iran war demonstrates how the type of leadership determines maneuvering through the maze of hybrid warfare. Both nations devised strategies and capabilities that were very different but effective in countering attacks from the other and exploiting their vulnerabilities (Eilam 2016; Smith 2020; Segell 2021). The skills needed for leadership in this digital age include the ability to use technology and understand human behavior (Hoffman, Neumeyer, and Jensen 2024), that is, drawing on big data analytics, strong artificial intelligence tools and similar high-end technologies for optimized decision making but also communicating with multiple community stakeholders in an unpredictable environment and using that skill to build trust (Tariq, et al. 2021). It is not a conventional war, but a hybrid war manifested in cyberattacks, targeted strikes, disinformation campaigns, and proxy operations. Israeli military leadership has shown agility in the high integration of technology, pre-emptive strategic doctrines, and real-time multi-agency coordination. Iran illustrates the use of proxy forces, asymmetric tactics, and digital influence operations as an adaptive structure, decentralized but ideologically anchored. These engagements show how adaptive leadership now transcends battlefields to the domains of psychology and the digital.

4. Institutional and Educational Imperatives for Cultivating Adaptive Military Leaders

Producing adaptive leaders requires, in fact, a total change in military education and culture through diverse strategic initiatives. That change is to prepare military personnel both in terms of skills and mindset to deal with the complexities of modern warfare within a context of fast technological development, hybrid threats, and irregular battlefields (Ryan 2020). Educational reform should focus more on critical thinking, problem-solving, and decision-making under uncertainty; moreover, it should promote continuous learning and adaptation. Three core pillars define this leadership paradigm*:*

Adaptability as a Strategic Imperative: The ability to respond quickly to changing conditions and the willingness to question old ways of doing things have become an imperative.

Continuous Learning as a Competitive Advantage: Because of the pace of technological and geopolitical change, leaders must be committed to learning for life, staying aware of new technologies and cross-cultural dynamics.

Resilience as a Foundation for Success: Psychological and emotional resilience supported by organizational support structures will be critical in sustaining performance under pressure.

By embedding these principles at the levels of education, training, doctrine, and organizational culture, military institutions will thereby produce leaders who can understand modern complexity better and more prepared generations to lead in today's conflicts (Albayrak and Ertürk 2021). Only through such holistic transformation can armed forces truly "win tomorrow's wars today."

4.1. Professional Military Education Reform: Integrating Digital Ethics, Systems Thinking, and Cross-Domain Operations

Conventional military education does not prepare commanders adequately to confront such multiple challenges in contemporary warfare. Reform of Professional Military Education (PME) means imparting digital ethics, systems thinking, and cross-domain operations to the curriculum (Woldenberg 2023). Digital ethics helps in understanding the emerging moral dilemmas that come with the use of AI and cyber capabilities; this ensures responsible use of technology (Chen, et al. 2024). Systems thinking will enable them to view how elements are interconnected within a system and thus anticipate some unintended consequences that can happen to make better decisions (Sun, et al. 2024). Cross-domain operations include land, sea, air, space, and cyberspace domains; therefore, leaders must learn how to integrate different domain resources for orchestrating synchronized operations in multiple domains.

4.2. Red Teaming and Scenario Simulations: Enhancing Decision-Making Under Ambiguity

Red teaming and scenario simulations are used, respectively, as complementary tools useful in making decisions amidst ambiguity and uncertainty. In red teaming, the team is tasked to challenge the plans and assumptions of an organization in a way that would identify vulnerabilities and weaknesses (Sun, Zhang, and Zhu 2022; UFMCS 2015). Scenario simulation creates a somewhat real situation where participants are forced to make decisions under pressure, thus practicing decision-making skills and learning from mistakes (Hoffman 2024). These build leaders who can think critically amid changing circumstances and make sound judgments with incomplete information.

Red teaming and scenario simulations help leaders to test their assumptions and discover any vulnerabilities in the process of decision-making under very realistic conditions, with pressures that might even intensify the actual climate of making decisions. The learning process, which involves an active challenge to established

wisdom and taking alternative viewpoints, creates for the leader a much more nuanced perception of complicated situations as well as heightened anticipation of possible developments that may indeed catch one by surprise. Even more genuine and effective is the merging of virtual reality and augmented reality technologies in such simulations whereby, within safe confines, participants can experience first-hand the fallout from their decision (Pleban, et al. 2002).

The combination of human skills and the use of AI-based tools will make for improved protection against attacks, showing how they form a tag team in today's security (Iyer 2024). Furthermore, across sectors, joint educational and training exercises help improve interoperability as well as integrated preparedness through methods like horizon scanning and decision theaters used for educating strategic analysts and training decision-makers (Knutsson and Mårtensson 2015). Even realistic cyberwarfare exercises that have been developed using a framework that emphasizes realism in environment, adversary, communications, tactics, and roles assure valuable, relevant training (Dobson, et al. 2017). These exercises are held with individuals from many different functional areas within an institution to be as close to a real experience of cyber-attack and response as possible (Colbert, Kott, and Knachel 2020). The same systems that organizations have employed to coordinate their crisis responses and deliver decision support can now be modified so as to simulate and game the real crises to rehearse appropriate responses (Walker, Giddings, and Armstrong 2011).

4.3. Interdisciplinary Learning: Blending Engineering, Political Science, and Behavioral Studies

Adaptive leadership calls for great familiarity with a wide range of disciplines, from engineering and political science to behavioral studies. Interdisciplinary learning makes the leader view technical, political, and human aspects; such holism allows the leader to perceive these three dimensions in the context of conflict (Lindsay and Friesen 2020). Such interdisciplinary learning draws keener insights from various fields, offering well-rounded, adaptive military leaders (Kochavi 2022). To that end, cross-disciplinary collaboration and knowledge sharing at military education institutions help realize more holistic understandings of complex challenges, thereby fostering innovative solutions. Military technology capability and constraints can be best judged by engineering knowledge (Krylova, et al. 2019). Political science sheds light on the political processes within which conflicts unfold as well as the interests motivating different actors (Horowitz 2020). Behavioral studies assist a leader in understanding how humans behave so that they might better influence or motivate their subordinates.

4.4. Leadership Labs: Creating Experimental Environments for Agile Command Exercises

In such leadership labs, an experimental environment is offered wherein agile command can be practiced. In a safe and secure environment, leaders get to sharpen their skills. Certainly, advanced technology would serve this purpose, virtual reality

or augmented reality simulation of the battlefield conditions (Uckelmann, et al. 2021). In it, participants can try out different styles and methods of leadership; feedback is provided on their performance, and they learn from the experience. Leadership labs foster a culture of experimentation and innovation in which leaders may challenge established wisdom about warfare and even create new approaches (Kjærgaard and Meier 2022).

4.5. Partnerships with Tech Sectors: Integrating Innovation Hubs and Defense Start-Ups into the Training Pipeline

Links to the tech sectors, pulling in innovation centers and defense start-ups into the training process, help share new ideas and methods (Watts, et al. 2023). These deals help get new technologies and skills so leaders can stay in front of changes that happen fast in a world of constant technological growth (Zervas and Stiakakis 2024). Innovation centers show a group helping link military people with scholars and industry professionals. Defense start-ups bring new ways to solve military problems; more often, they bring new thoughts and different ways. This teamwork is most important for keeping a lead in today's digital world (Steiro and Torgersen 2020). The combination of these teaching methods helps military leaders become flexible and good at dealing with the tricky modern times. This also allows leaders to successfully bring in new technologies, think deeply, and create a workplace culture that encourages new ideas (Bresler 2018). These institutional and educational mandates together produce adaptive leaders capable of operating effectively in chaos and helping to define the future of conflict. Through these reforms, military organizations would develop an adaptability culture, a learning culture, and a resilience culture—well-prepared to take on the new challenges of the 21st century.

5. Recommendations for Building Future Commanders: Institutionalizing Adaptive Leadership

To really make adaptive leadership a part of military groups, there is a need to take many steps all at once and bring about changes in doctrine, hand over more decision-making power, spend on ethical-AI training, build feedback cultures, and make sure leadership growth matches strategic foresight (Joshi 2025; Liseanu 2023). These tips together try to build a nimbler, stronger, and more creative military force that can deal with the challenges of today's warfare.

5.1. Update Doctrine: Reflect the Realities of AI, Cyber, and Hybrid Warfare

Military doctrine should reflect the metamorphic impact of AI, cyber operations, and hybrid warfare. Doctrines are often inadequate in addressing new challenges, and that is their great weakness. In turn, new doctrines should guide ethical and legal frameworks for AI in War alongside strategies for cyber defense and measures to counter disinformation (Taddeo, et al. 2022). They should also advance the principles of hybrid warfare, which is the integration of conventional and unconventional methods of achieving strategic ends.

5.2. Decentralized Decision-Making: Train Mid-Level Leaders to Act with Autonomy

In today's rapidly evolving operational environment, centralized decision-making can be a bottleneck. Decentralizing decision-making empowers mid-level leaders to act with autonomy, enabling them to respond quickly and effectively to changing circumstances (Mittal 2018). This requires providing mid-level leaders with the necessary training, resources, and authority to make decisions on their own initiative (De Smet, Hewes, and Weiss 2020). It also requires fostering a culture of trust and empowerment, where leaders are encouraged to take risks and learn from their mistakes.

5.3. Invest in Ethical-AI Training: Prepare Commanders for Moral Dilemmas

The increasing use of AI in warfare raises significant ethical concerns. Military organizations must invest in ethical AI-training to prepare commanders for the moral dilemmas they may face when using AI-powered systems (Taddeo, et al. 2022). This training should cover topics such as bias in AI algorithms, the potential for unintended consequences, and the responsibility for the actions of autonomous weapons systems. It should also emphasize the importance of human oversight and accountability (Davidovic 2023).

5.4. Create Feedback Cultures: Promote Reflection, Iteration, and Innovation

A culture of feedback is essential for promoting reflection, iteration, and innovation within military organizations. Leaders should actively solicit feedback from their subordinates, peers, and superiors (Lythgoe 2024). They should also be open to criticism and willing to learn from their mistakes. Feedback should be used to identify areas for improvement and to develop new and better ways of doing things. Furthermore, organizations should create mechanisms for sharing best practices and lessons learned across different units and departments.

5.5. Align Leadership Development with Strategic Foresight: Use Future Scenarios to Shape Current Practices

Leadership development should be aligned with strategic foresight, using future scenarios to shape current practices. This involves identifying potential future threats and challenges and developing leaders who are capable of anticipating and responding to them. Scenario planning exercises can be used to explore different future scenarios and to identify the skills and capabilities that will be needed to succeed in each scenario (Rhoods and Babor 2018; Star, et al. 2016). This information can then be used to develop leadership development programs and to ensure that leaders are prepared for the challenges of the future. By implementing these recommendations, military organizations can cultivate a culture of adaptive leadership, ensuring that they are well-prepared to meet the challenges of the 21st century (Akturan 2024). This will involve a continuous process of learning, adaptation, and innovation, as the nature of warfare continues to evolve.

Conclusions

The increasing complexity of modern warfare calls for a change in military leadership. As discussed in this paper, future adaptive leadership, which entails strategic flexibility, operational agility, and technological fluency, is increasingly becoming the determinant of effectiveness in the digitalized world. From comparison across Ukraine's war, Nagorno-Karabakh's conflict, and Israel–Iran's hybrid confrontation, one finds that institutional as well as immediate adaptation does not give room for a preponderance but rather ensures survival.

The Ukrainian case shows how a military organization under severe resource constraints can generate asymmetric advantages through decentralization, fast digital integration, and creative applications of commercially available technologies. Ukraine's success in maintaining resilience in operations and disruption against a much more powerful adversary demonstrates how adaptive leadership can reconfigure the balance of power through innovation and improvisation and by empowering tactical-level commanders.

In the 2020 Nagorno-Karabakh war, Azerbaijan perfected the art of combining drone warfare with ISR integration, and ground forces joined digitally — a fact not very much appreciated. It was not just a matter of technological superiority but rather having the foresight to strategically reposition traditional tactics on the basis of real-time data as well as narrative control. This example does reaffirm that adaptive leadership is more than just responding to change – it is about getting ahead in the process of shaping the tempo, perception, and outcomes of conflict.

The Israel–Iran confrontation represents the evolution of warfare into a hybrid landscape in which military engagements become deeply intertwined with cyber operations, proxy networks, and information warfare. In this sense, organizational adaptability can be defined as the ability of a state to carry out multi-agency preemptive actions enabled by technology. On the other hand, organizational adaptability can also mean the capacity to use decentralized proxies, asymmetric tactics, and influence operations like Iran's to avoid direct confrontation – and to exploit ambiguity in any system. Therefore, adaptive leadership by both Israelis and Iranians must move beyond the battlefield into the digital, cognitive, and informational spaces.

It is in the pattern of military organizations that foster initiative, decentralize authority, and institutionalize learning that assist best navigation in a volatile and uncertain environment. Leadership in Digital Age Operations does not lead from the front or by technical expertise but requires synthesizing information, anticipating disruption, and leading evolving systems under pressure. The study brings out clearly

how adaptive leadership moves from being a theoretical construct to an operational imperative in contemporary security environments. It further shifts the emphasis onto dynamic leaders and institutions rather than static doctrine as determinants of future military effectiveness. Cultivation of adaptability at all echelons of command as warfare moves across physical, digital, and psychological spaces will be not only a determinant of tactical success but also an enabler of strategic endurance.

Recommendations for Future Research

While this work initiates an inquiry into adaptive military leadership in the digital age, further queries remain:
Future studies need to render factors such as cognitive agility, ethical reflexivity, and resilience within military cohorts measurable to quantitatively assess their impact on decision-making effectiveness under stress as well as on the group.

Adaptive leadership will manifest differently in centralized versus decentralized structures. Therefore, comparative analyses between NATO members, emerging powers, and hybrid warfare practitioners (such as Ukraine, Azerbaijan, and Israel) will reveal the contextual factors at play in successful adaptation.
As curricula integrate AI literacy, systems thinking, and digital ethics, longitudinal studies will be needed to determine whether such curricula measurably increase leadership adaptability in deployments.

Future research should explore how AI-generated battlefield insights influence leadership judgment, especially in ambiguous ethical scenarios. This includes studies on human-in-the-loop systems and the psychological effects of AI-assisted command.
Experimental environments using VR/AR and red teaming should be systematically studied to determine how immersive training affects adaptive capacity, ethical reasoning, and strategic foresight among officers.

The adaptive leadership approach is under consideration in multinational and joint operations, with further emphasis on how adaptive leadership translates across cultural and doctrinal lines, given NATO's greater emphasis on interoperability. This will enable scholars and defense practitioners to jointly advance a general theory of adaptive military leadership that is both intellectually rigorous and practically consequential in shaping leaders for the conflicts of the 21st century by broadening empirical inquiry.

References

Achuthan, K., S. Ramanathan, S. Srinivas and R. Raman. 2024. "Advancing cybersecurity and privacy with artificial intelligence: current trends and future research directions." *Frontiers in Big Data* 7. https://doi.org/10.3389/fdata.2024.1497535

Akturan, A. 2024. "Yapay Zekânın İşletme Yönetimi ve Liderlik Üzerindeki Etkileri: Bir Literatür İncelemesi." *Sinop Üniversitesi Sosyal Bilimler Dergisi* 8(2): 1305-1348. https://doi.org/10.30561/sinopusd.1554856

Albayrak, M. T., and A. Ertürk. 2021. "Strategic Empowerment in Human Resource Management." In *Oxford Research Encyclopedia of Business and Management*.

Antoniuk, L., & V. Zasiadivko. 2023. "Digital literacy and technologies for education: principles and tools." *Grail of Science* 26: 249-252. https://doi.org/10.36074/grail-of-science.14.04.2023.044

Arasli, J. 2007. *Obsolete weapons, unconventional tactics, and martyrdom zeal: How Iran would apply its asymmetric naval warfare doctrine in a future conflict.* https://www.marshallcenter.org/sites/default/files/files/2019-07/PDF_PUB_OPS_10.pdf

Ardiansyah, S. 2025. *Anticipating the Future of Drone Warfare: Trends, Implications, and Challenges.* https://sendyardiansyah.medium.com/anticipating-the-future-of-drone-warfare-trends-implications-and-challenges-d6cffb1ee1b6

Askew, N. P. 2023. "Leading With Principle: The Essential Role of Ethical Leadership in Adaptive Environments." *Journal of Leadership, Accountability & Ethics* 20(5). https://doi.org/10.33423/jlae.v20i5.6605

Baccino L., O. Desilles, L. Kille, and J. Raggio. 2025. *Imminent Warning: Iranian Retaliation, Increased Regional Tensions, and Growing Antisemitism Expected After IS.* https://www.counterterrorismgroup.com/post/imminent-warning-iranian-retaliation-increased-regional-tensions-and-growing-antisemitism-expecte

Bailey, D. E., S.L. Docherty, J.A. Adams, D.L. Carthron, K. Corazzini, J.R. Day, E. Neglia, M. Thygeson, and R.A. Anderson. 2012. "Studying the clinical encounter with the Adaptive Leadership framework." *Journal of Healthcare Leadership, 83.* https://doi.org/10.2147/jhl.s32686

Bankins, S., A.C. Ocampo, M. Marrone, S.L.D. Restubog and S.E. Woo. 2024. "A multilevel review of artificial intelligence in organizations: Implications for organizational behavior research and practice." *Journal of organizational behavior* 45(2): 159-182. https://doi.org/10.1002/job.2735

Baram, G., and I. Ben-Israel. 2025. "Redefining vigilance: reevaluating the meaning of early warning in Israel's security doctrine and the October 7 attack." *Intelligence and National Security*, 1-16. https://doi.org/10.1080/02684527.2025.2466267

Beckner, M. E., W.R. Conkright, S.R. Eagle, B.J. Martin, A.M. Sinnott, A.D. LaGoy, ... and B.C. Nindl. 2021. "Impact of simulated military operational stress on executive function relative to trait resilience, aerobic fitness, and neuroendocrine biomarkers." *Physiology & behavior,* 236. https://doi.org/10.1016/j.physbeh.2021.113413

Beretas, C. 2020. "Cyber Hybrid Warfare: Asymmetric threat." *Nanotechnol Adv Mater Sci* 3(1): 1-2. https://doi.org/10.32474/mams.2020.02.000151

Boikanyo, D. H. 2025. "Adaptive Leadership in Times of Organizational Change Driven by Digital Technologies." *Contemporary Perspectives on Organizational Behaviour*, 37. https://doi.org/10.5772/intechopen.1007826

Bresler, A. 2018. "Improving defense innovation programs to enhance force readiness." *Journal of Defense Analytics and Logistics* 2(2): 110-124. https://doi.org/10.1108/jdal-06-2018-0010

Caro, C.J.V. 2025. *Enduring Defeat: The Cyclical Failures of Russian Military Culture.* https://www.realcleardefense.com/articles/2025/03/10/enduring_defeat_the_cyclical_failures_of_russian_military_culture_1096481.html

Chen, Z., C. Chen, G. Yang, X. He, X. Chi, Z. Zeng, and X. Chen. 2024. "Research integrity in the era of artificial intelligence: Challenges and responses." *Medicine* 103(27): e38811. https://doi.org/10.1097/md.0000000000038811

Chernobrov, D. 2025. "Participatory propaganda and the intentional (re) production of disinformation around international conflict." *Critical Studies in Media Communication* 42(1): 101-106. https://doi.org/10.1080/15295036.2025.2467433

Cheterian, V. 2022. "Technological determinism or strategic advantage? Comparing the two Karabakh Wars between Armenia and Azerbaijan." *Journal of Strategic Studies* 47(2): 214-237. https://doi.org/10.1080/01402390.2022.2127093

Clark, B., D. Patt, and T.A. Walton. 2021. *Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage*. Hudson Institute. https://www.hudson.org/national-security-defense/implementing-decision-centric-warfare-elevating-command-and-control-to-gain-an-optionality-advantage

Clarke, R.A. 2024. "Hostile State Disinformation in the Internet Age." *Daedalus* 153(3): 45-64. https://doi.org/10.1162/daed_a_02088

Colbert, E.J., A. Kott, and L.P. Knachel. 2020. "The game-theoretic model and experimental investigation of cyber wargaming." *The Journal of Defense Modeling and Simulation* 17(1): 21-38. https://doi.org/10.1177/1548512918795061

Congressional Research Service. 2021. *Iran's Foreign and Defense Policies.* https://fas.org/sgp/crs/mideast/R44017.pdf

Cornell, S.E. 2017. *The Armenian-Azerbaijani Conflict and European Security* (pp. 1-21). Palgrave Macmillan US. https://link.springer.com/chapter/10.1057/978-1-137-60006-6_1

Crayne, R. 2025. *Our Most Powerful Weapon: The Army Ethic.* https://www.ausa.org/publications/harding-paper/our-most-powerful-weapon

Crivellaro, J.C. 2013. *Combined Arms in the Electro-Magnetic Spectrum: Integrating Non-kinetic Operations.* https://apps.dtic.mil/dtic/tr/fulltext/u2/a583814.pdf

Crowley, T. 2025. *Bayraktar TB2.* https://www.nsin.us/bayraktar-tb2/

Center for Strategic & International Studies (CSIS). 2025. *Ungentlemanly Robots: Israel's Operation Rising Lion and the New Way of War.* https://www.csis.org/analysis/ungentlemanly-robots-israels-operation-rising-lion-and-new-way-war

Daly, J. 2025. *How Starlink Keeps Ukraine's Military Online and Ahead in Battle.* https://united24media.com/war-in-ukraine/how-starlink-keeps-ukraines-military-online-and-ahead-in-battle-6797

Davidovic, J. 2023. "On the purpose of meaningful human control of AI." *Frontiers in big data*, *5*. https://doi.org/10.3389/fdata.2022.1017677

De Smet, A., C. Hewes, and L. Weiss. 2020. *For smarter decisions, empower your employees.* https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/for-smarter-decisions-empower-your-employees

Deep, G. 2023. "The power of resilience and flexibility in business leadership: Adapting to change." *Magna Scientia Advanced Research and Reviews*, *9*(2): 86-91. https://doi.org/10.30574/msarr.2023.9.2.0164

Demus, A., K. Holynska, and K. Marcinek. 2023. *The Nightingale Versus the Bear: What Persuasion Research Reveals About Ukraine's and Russia's Messaging on the War*. RAND. https://doi.org/10.7249/rra2032-1

Deppe, C., and G.S. Schaal. 2024. "Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept." *Frontiers in Big Data*, 7. https://doi.org/10.1080/02564602.2003.11417080

Dhopte, A., and H. Bagde. 2023. "Smart smile: revolutionizing dentistry with artificial intelligence." *Cureus* 15(6): e41227. https://doi.org/10.7759/cureus.41227

Dias, V. 2024. The *Art of Delegation: Empowering and Engaging Employees through Effective Leadership.* https://www.linkedin.com/pulse/art-delegation-empowering-engaging-employees-through-effective-dias-sdjaf

Dickinson, P. 2022. *The Ukrainian military must reorganize to defeat Russia.* https://www.atlanticcouncil.org/blogs/ukrainealert/the-ukrainian-military-must-reorganize-to-defeat-russia/

Dobson, G.B., T.G. Podnar, A.D. Cerini, and L.J. Osterritter. 2017. "R-eactr: A framework for designing realistic cyber warfare exercises." *Software Engineering Institute, Pittsburgh, PA*. https://apps.dtic.mil/sti/pdfs/AD1044880.pdf

Edmonds, J., S. Bendett, A. Fink, M. Chesnut, D. Gorenburg, M. Kofman, ... and J. Waller. 2021. *Artificial intelligence and autonomy in Russia*. CNA. https://www.cna.org/analyses/2021/05/ai-and-autonomy-in-russia

Eilam, E. 2016. "The struggle against Hizbullah and Hamas: Israel's next hybrid war." *Israel Journal of Foreign Affairs* 10(2): 247-255. https://doi.org/10.1080/23739770.2016.1207130

Ertürk, A., and T. Albayrak. 2020. "Empowerment and organizational identification: The mediating role of leader–member exchange and the moderating role of leader trustworthiness." *Personnel Review* 49(2): 571-596. https://doi.org/10.1108/PR-02-2018-0054

Epstein, O., G.D. Perkin, J. Cookson, I.S. Watt, R. Rakhit, A.W. Robinson, G.A.W. Hornett. 2008. Clinical examination. 4th edn. Oxford: Mosby Elsevier.

Faro, M. 2024. *Brass tacks: Why Russia's military fails to reform.* https://ecfr.eu/publication/brass-tacks-why-russias-military-fails-to-reform/

Feldman, P., A. Dant, and A. Massey. 2019. *Integrating artificial intelligence into weapon systems.* https://doi.org/10.48550/arXiv.1905.03899

Frappi, C. 2023. Armenia 2022: "Looking for a way out of the Nagorno-Karabakh impasse." *Asia Maior*, *33:* 447-477. https://doi.org/10.52056/979125463667/19

Good, D. 2014. "Predicting real-time adaptive performance in a dynamic decision-making context." *Journal of Management & Organization* 20(6): 715-732. https://doi.org/10.1017/jmo.2014.54

Hagos, D. H., and D.B. Rawat. 2022. "Recent advances in artificial intelligence and tactical autonomy: Current status, challenges, and perspectives." *Sensors*, *22*(24), 9916. https://doi.org/10.3390/s22249916

Harper C. and R.B. Cross. 2024. *NATO must recognize the potential of open-source intelligence.* https://www.atlanticcouncil.org/blogs/new-atlanticist/nato-must-recognize-the-potential-of-open-source-intelligence/

Heifetz, R., A. Grashow, and M. Linsky. 2009. " Leadership in a (permanent) crisis." *Harvard business review* 87(7/8): 62-69. https://pubmed.ncbi.nlm.nih.gov/19630256

Herrero Ocasar, D., and W. Suengkamolpisut. 2005. "The Emotionally Intelligent Leader.

Hoffman, J. 2024. Enhancing community engagement in scenario-based urban planning and policy development using experiential futures." *Journal of Urbanism International Research on Placemaking and Urban Sustainability, 1-26.* https://doi.org/10.1080/17549175.2024.2307049

Hoffman, F., M. Neumeyer, and B. Jensen. 2024. *The Future of Hybrid Warfare.* https://www.csis.org/analysis/future-hybrid-warfare

Horowitz, M. C. 2019. "When Speed Kills: Autonomous Weapon Systems, Deterrence, and Stability." *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.3348356

___. 2020. "Do emerging military technologies matter for international politics?" *Annual Review of Political Science* 23(2020): 385-400. https://doi.org/10.1146/annurev-polisci-050718-032725

Hozint.com. 2025. *Operation Rising Lion: Israel's Strike on Iran's Nuclear Facilities.* https://www.hozint.com/2025/06/operation-rising-lion-israels-strike-on-irans-nuclear-facilities/

Huettermann, H., S. Berger, M. Reinwald, and H. Bruch. 2024. "Power to the people—And then? A multilevel leadership perspective on organizational decentralization." *Human Resource Management* 63(2): 333-353. https://doi.org/10.1002/hrm.22203

Hwang, S., and S.J. Joo. 2023. "Examining the impact of the COVID-19 pandemic on container carrier performance." *Maritime Economics & Logistics*, 1. https://doi.org/10.1057/s41278-023-00260-2

Iskandarov, K., and P. Gawliczek. 2021. "Characteristic features of the second Karabakh war." *Social Development and Security* 11(3): 30-40. https://doi.org/10.33445/sds.2021.11.3.3

Iyer, K.N. 2024. "AI and Human Analysts: The Ultimate Synergy for Threat Defense." *International Journal of Innovative Research in Computer and Communication Engineering 12(4).* https://doi.org/10.15680/ijircce.2024.1204372

Jnitova, V., K. Joiner, M. Efatmaneshnik, and E. Chang. 2021. "Modelling workforce employability pipelines for organisational resilience." *International Journal of Engineering Business Management,* 13. https://doi.org/10.1177/18479790211004010

Johnco, C., V.M. Wuthrich, and R.M. Rapee. 2013. "The role of cognitive flexibility in cognitive restructuring skill acquisition among older adults." *Journal of Anxiety disorders* 27(6): 576-584. https://doi.org/10.1016/j.janxdis.2012.10.004

Joshi, S. 2025. *Leadership in the age of AI: Review of quantitative models and visualization for managerial decision-making.* https://doi.org/10.2139/ssrn.5223882

Kahn, L. 2022. "How Ukraine is remaking war. Technological advancements are helping Kyiv succeed." *Foreign Affairs*, 29. https://www.foreignaffairs.com/ukraine/how-ukraine-remaking-war

Khalilzada, J. 2024. "Does the Offence–Defence Theory Explain War Onset Between Small States? Causes and Consequences of the 2020–2023 Armenia–Azerbaijan War." *Journal of Asian Security and International Affairs* 11(2): 190-213. https://doi.org/10.1177/23477970241250099

Kjærgaard, A., and F. Meier. 2022. "Trying out loud: Leadership development as experimentalism." *Leadership* 18(3): 383-399. https://doi.org/10.1177/17427150211063381

Knutsson, R., P.Å. Mårtensson, E. Brattberg, and L. Hedström. 2015. "Bio-Agro Defense Collaboration: The Need of Joint Leadership Education and Training of Strategic Analysts and Decision Makers." *J Def Manag* 5(131): 2167-0374. https://doi.org/10.4172/2167-0374.1000131

Kochavi, A. 2022. *To Be a Military Leader.* https://www.idf.il/en/mini-sites/dado-center/research/to-be-a-military-leader-major-general-kochavi/

Kot, S., A. Mozolevska, O. Polishchuk, and Y. Stodolinska. 2024. "The discursive power of digital popular art during the Russo-Ukrainian War: Re/shaping visual narratives." *Arts* 13(1): 38. MDPI. https://doi.org/10.3390/arts13010038

Kott, A., D.S. Alberts, and C. Wang. 2015. *War of 2050: a battle for information, communications, and computer security.* Cornell University. https://doi.org/10.48550/arXiv.1512.00360

Koukoudakis, G. 2024. "Drones' contribution to the transformation of contemporary warfare." *Journal of Military Studies* 13(1): 24-32. https://doi.org/10.2478/jms-2024-0003

Krylova, I.V., I.A. Medianik, V.Y. Mekhanikov, R.A. Panarin, E.V. Polikarpova, and D.S. Uleschenko. 2019. "New aspects of russian national security system in the conditions of peaceful war." *Humanities and Social Sciences Reviews* 7(5): 725-730. https://doi.org/10.18510/hssr.2019.7589

Kudlenko, A. 2023. "Roots of Ukrainian resilience and the agency of Ukrainian society before and after Russia's full-scale invasion." *Contemporary Security Policy* 44(4): 513-529. https://doi.org/10.1080/13523260.2023.2258620

Kushnir, V., and O. Chernobai. 2020. "Features of the Organization of Work of Public Affairs Divisions of The Ministry of Defence of Ukraine During the Armed Aggression of The Russian Federation Against Ukraine." *Krakowskie Studia Małopolskie* 2: 119-134. https://doi.org/10.15804/ksm20200208

Lindsay, D.R., and K.L. Friesen. 2020. "Interdisciplinary Leadership: Collectively Driving the Field Forward: Priority 7 of the National Leadership Education Research Agenda 2020–2025." *Journal of Leadership Studies* 14(3): 78-81. https://doi.org/10.1002/jls.21715

Liseanu, R. 2023. "The Modern Military Leadership – The Anchor of Organizational Culture in the Contemporary World." *Revista Academiei Forţelor Terestre 28(2): 80-87.* https://doi.org/10.2478/raft-2023-0011

Lythgoe, T.J. 2024. *Future Proof: How to Build a Learning Organization.* https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2024-OLE/Future-Proof/

Matli, W. 2024. "Integration of warrior artificial intelligence and leadership reflexivity to enhance decision-making." *Applied Artificial Intelligence* 38(1): 2411462. https://doi.org/10.1080/08839514.2024.2411462

Mejova, Y., A. Capozzi, C. Monti, and G.D.F. Morales. 2023. *Narratives of War: Ukrainian Memetic Warfare on Twitter. Cornell University.* https://doi.org/10.48550/arXiv.2309.08363

Meriläinen, N. 2025. "Influencers as Tools in Hybrid Operations Online." In *International Conference on Cyber Warfare and Security* (pp. 265-272). Academic Conferences International. https://doi.org/10.34190/iccws.20.1.3187

Mikayılov, T.N., and A.A. oğlu Bayramov. 2019. "The Possibility of Creating an Automated Control System of The Various Military Groups." *Advanced Information Systems* 3(3): 25-29. https://doi.org/10.20998/2522-9052.2019.3.03

Mittal, K. 2018. "Impact of Leadership styles on employees' performance: An empirical investigation of Middle-Level employees." *Psychol. Educ.* 55(1): 452-460. https://doi.org/10.48047/pne.2018.55.1.56

Moreno, J.C.A. 2021. "Understanding the Operational Environment: The human dimension." *Global strategy reports*, No. 1. https://dialnet.unirioja.es/servlet/articulo?codigo=7771668

Nalin, L.C.A., and P. Tripodi. 2023. "Future warfare and responsibility management in the AI-based military decision-making processs." *Journal of Advanced Military Studies* 14(1): 83-97. https://doi.org/10.21140/mcuj.20231401003

Navaratna, A. R. 2025. *Digital Transformation in Joint Warfighting.* https://cenjows.in/digital-transformation-in-joint-warfighting-a-digital-twin-use-case/

Nikolaou, I., A. Gouras, M. Vakola, and D. Bourantas. 2007. "Selecting change agents: Exploring traits and skills in a simulated environment." *Journal of Change Management* 7(3-4): 291-313. https://doi.org/10.1080/14697010701779173

Nyemann, D.B., and H. Sørensen. 2019. *MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare: A Multinational Capability Development Campaign project.* http://www.forskningsdatabasen.dk/catalog/2444108744

Pahlavi, P.C., and E. Ouellet. 2012. "Institutional analysis and irregular warfare: Israel Defense Forces during the 33-Day War of 2006." *Small Wars & Insurgencies* 23(1): 32-55. https://doi.org/10.1080/09592318.2012.632854

Pak, K., M.S. Polikoff, L.M. Desimone, and E. Saldívar García. 2020. "The adaptive challenges of curriculum implementation: Insights for educational leaders driving standards-based reform." *Aera Open* 6(2). https://doi.org/10.1177/2332858420932828

Papersowl.com. 2023. *Navigating Leadership through ADP 6-22.* https://papersowl.com/examples/navigating-leadership-through-adp-6-22/

Pashayeva, G.N. 2023. *Emergence and development stages of informatics in Azerbaijan.* https://doi.org/10.25045/jpis.v15.i1.08

Pleban, R.J., M.D. Matthews, M.S. Salter and D.E. Eakin. 2002. "Training and assessing complex decision-making in a virtual environment." *Perceptual and Motor Skills* 94(3): 871-882. https://doi.org/10.2466/pms.2002.94.3.871

Porkoláb, I. 2020. "An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges." In *Artificial Intelligence and Global Security* (pp. 153-165). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-811-720201009

Pretto, A., S. Aravecchia, W. Burgard, N. Chebrolu, C. Dornhege, T. Falck, ... and J. Nieto. 2020. "Building an aerial–ground robotics system for precision farming: an adaptable solution." *IEEE Robotics & Automation Magazine* 28(3): 29-49. https://doi.org/10.1109/mra.2020.3012492

Raska, M. 2019. *The SAF After Next Incarnation.* https://dr.ntu.edu.sg/bitstream/10356/106416/1/CO19041.pdf

Raugh, D.L. 2016. "Is the hybrid threat a true threat?" *Journal of Strategic Security* 9(2): 1-13. https://doi.org/10.5038/1944-0472.9.2.1507

Repost.press. 2025. *Future of the National Security Doctrine of Israel.* https://en.repost.press/news/future-of-the-national-security-doctrine-of-israel

Rhoods, S., and A. Babor. 2018. " The future of global research: A case study on the use of scenario planning in the publishing industry." *Learned Publishing* 31(3): 254-260. https://doi.org/10.1002/leap.1152

Robinson, K., B. McKenna, and D. Rooney. 2022. "The relationship of risk to rules, values, virtues, and moral complexity: What we can learn from the moral struggles of military leaders." *Journal of Business Ethics* 179(3): 749-766. https://doi.org/10.1007/s10551-021-04874-5

Roshanaei, M. 2021. "Resilience at the core: critical infrastructure protection challenges, priorities and cybersecurity assessment strategies." *Journal of Computer and Communications* 9(8): 80-102. https://doi.org/10.4236/jcc.2021.98006

Rustamzade, A., and A. Valiyev. 2024. *Drones and Special Forces: Armenian-Azerbaijani Relations in the Wake of the Second Karabakh War.* https://bakudialogues.ada.edu.az/articles/drones-and-special-forces-27-01-2022

Ryan, M. 2020. *The Intellectual Edge: A Competitive Advantage for Future War and Strategic Competition.* https://apps.dtic.mil/sti/pdfs/AD1104926.pdf

Saikal, A., and D. Vestenskov. 2020. " Iran's national security and operational capability." *Scandinavian Journal of Military Studies* 3(1). https://doi.org/10.31374/sjms.29

Sanders, D. 2023. "Ukraine's third wave of military reform 2016–2022–building a military able to defend Ukraine against the Russian invasion." *Defense & Security Analysis* 39(3): 312-328. https://doi.org/10.1080/14751798.2023.2201017

Segell, G. 2021. "Consistency of Civil-Military Relations in the Israel Defense Forces: The Defensive Mode in Cyber." *Journal of Advanced Military Studies* 12(1): 86-111. https://doi.org/10.21140/mcuj.20

Simpson, J., R. Oosthuizen, S.E. Sawah, and H. Abbass. 2021. *Agile, antifragile, artificial-intelligence-enabled, command and control.* https://doi.org/10.48550/arXiv.2109.06874

Smith, C.B. 2020. *The Quds Force Model: What Makes Irregular Warfare Effective in Asymmetric Conflict* (Doctoral dissertation, Monterey, CA; Naval Postgraduate School). https://apps.dtic.mil/sti/pdfs/AD1127101.pdf

Smith, J.D. Jr. 2024. *Cognitive Resilience in High-Stress Military Operations: Strategies and Implications.* https://www.psychbreakthrough.com/breakthrough-blog/cognitive-resilience-in-high-stress-military-operations-strategies-and-implications

Sobb, T., B. Turnbull, and N. Moustafa. 2023. "A holistic review of cyber–physical–social systems: New directions and opportunities." *Sensors* 23(17): 7391. https://doi.org/10.3390/s23177391

Sott, M. K., and M.S. Bender. 2025. "The Role of Adaptive Leadership in Times of Crisis: A Systematic Review and Conceptual Framework." *Merits* 5(1), 2. https://doi.org/10.3390/merits5010002

Sriharan, A., A.J. Hertelendy, J. Banaszak-Holl, M.M. Fleig-Palmer, C. Mitchell, A. Nigam, … and S.J. Singer. 2022. "Public health and health sector crisis leadership during pandemics: a review of the medical and business literature." *Medical Care Research and Review* 79(4): 475-486. https://doi.org/10.1177/10775587211039201

Star, J., E.L. Rowland, M.E. Black, C.A. Enquist, G. Garfin, C.H. Hoffman, ... and A.M. Waple. 2016. "Supporting adaptation decisions through scenario planning: Enabling the effective use of multiple methods." *Climate Risk Management* 13, 88-94. https://doi.org/10.1016/j.crm.2016.08.001

Steiro, T.J., and G.E. Torgersen. 2020. "Preparedness and multiagency collaboration—Lessons learned from a case study in the Norwegian Armed Forces." *Sustainability* 12(18): 7240. https://doi.org/10.3390/su12187240

Sun, N., Y. Miao, H. Jiang, M. Ding, and J. Zhang. 2024. *From Principles to Practice: A Deep Dive into AI Ethics and Regulations.* https://doi.org/10.48550/arxiv.2412.04683

Sun, S. L., Y. Zhang, and Z. Zhu. 2022. "Turning disruption into growth opportunity: the red team strategy." *Journal of Business Strategy* 43(6): 365-372. https://doi.org/10.1108/jbs-05-2021-0087

Tabansky, L. 2020. "Israel Defense Forces and National Cyber Defense." *Connections The Quarterly Journal 19(1): 45-62.* https://doi.org/10.11610/connections.19.1.05

Taddeo, M., D. McNeish, A. Blanchard and E. Edgar. 2022. *Ethical principles for artificial intelligence in national defence.* In *The 2021 Yearbook of the Digital Ethics Lab* (pp. 261-283). Cham: Springer International Publishing. https://doi.org/10.1007/s13347-021-00482-3

Tamburrini, G. 2021. *Digital Humanism and Global Issues in Artificial Intelligence Ethics. In Springer eBooks (p. 83). Springer Nature.* https://doi.org/10.1007/978-3-030-86144-5_12

Tariq, M. U., M. Babar, M. Poulin, A.S. Khattak, M.D. Alshehri, and S. Kaleem. 2021. "Human behavior analysis using intelligent big data analytics." *Frontiers in Psychology*, 12. https://doi.org/10.3389/fpsyg.2021.686610

Teixeira, J., L. Pais, N.R. dos Santos, and B. Sousa. 2024. "Empowering Leadership in the Military: Pros and Cons." *Merits* 4(4): 346-369. https://doi.org/10.3390/merits4040026

Thakur, K., and A.K. Pathan. 2020. *Cybersecurity Basics*. In *CRC Press eBooks (p. 31)*. Informa. https://doi.org/10.1201/9781003035626-2

Türk, A. 2023. "Digital leadership role in developing business strategy suitable for digital transformation." *Frontiers in psychology* 13: 1066180. https://doi.org/10.3389/fpsyg.2022.1066180

Uckelmann, D., D. Mezzogori, G. Esposito, M. Neroni, D. Reverberi, M. Ustenko, and J. Baalsrud-Hauge. 2021. "Guideline to safety and security in federated remote labs." *International Journal of Online and Biomedical Engineering* 17(4): 39-62. https://doi.org/10.3991/ijoe.v17i04.18937

Uddin, A. A. 2023. "The era of AI: Upholding ethical leadership." *Open Journal of Leadership* 12(4): 400-417. https://doi.org/10.4236/ojl.2023.124019

University of Foreign Military and Cultural Studies (UFMCS). 2015. *The Applied Critical Thinking Handbook.* https://irp.fas.org/doddir/army/critthink.pdf

Walker, W.E., J. Giddings, and S. Armstrong. 2011. "Training and learning for crisis management using a virtual simulation/gaming environment." *Cognition, Technology & Work* 13, 163-173. https://doi.org/10.1007/s10111-011-0176-5

Watling, Jack, and Nick Reynolds. 2022. *Ukraine at War: Paving the Road From Survival to Victory.* https://rusi.org/explore-our-research/publications/special-resources/ukraine-war-paving-road-survival-victory

Watts, S., B. Frederick, N. Chandler, M. Toukan, C. Curriden, E.E. Mueller, E. Geist, A.M. Tabatabai, S. Plana, B. Corbin, and J. Martini. 2023. *Proxy Warfare in Strategic Competition: Military Implications. In RAND Corporation eBooks.* https://doi.org/10.7249/rra307-3

Weidman, N. 2021. *Killer instinct: The popular science of human nature in twentieth-century America*. Harvard University Press. https://doi.org/10.4159/9780674269651

Woldenberg, W.L. 2023. *End the Professional Military Education Equivalency Myth.* https://www.armyupress.army.mil/journals/military-review/online-exclusive/2023-ole/woldenberg/

Wu, M. 2022. *Cyberspace Operations. In Routledge eBooks (p. 240). Informa.* https://doi.org/10.4324/b22974-11

Zanglin, L. 2017. *Air Sigma Model of Leadership.* https://doi.org/10.2139/ssrn.2962019

Zakharchenko, A. 2025. "Advantages of the connective strategic narrative during the Russian–Ukrainian war." *Frontiers in Political Science*, 7. https://doi.org/10.3389/fpos.2025.1434240

Zervas, I., and E. Stiakakis. 2024. "Economic Sustainable Development through Digital Skills Acquisition: The Role of Human Resource Leadership." *Sustainability* 16(17): 7664. https://doi.org/10.3390/su16177664

FUNDING INFORMATION
N/A

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 that support the findings of this study are openly available on the internet.

DECLARATION on AI use (if applicable)
N/A

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Doctrinal and Tactical Aspects of Deploying Anti-Tank Guided Missile Platoons in Defence

CPT Marko RADOVANOVIC, MSc*
LTC Misa ZIVKOVIC, MSc**
LTC Aleksandar PETROVSKI, PhD***
LT Rexhep MUSTAFOVSKI, MSc****

*University of Defence, Military Academy, Belgrade, Serbia
e-mail: markoradovanovicgdb@yahoo.com
**University of Defence, Military Academy, Belgrade, Serbia
e-mail: zivkovic.misa@yahoo.com
***Goce Delcev University' Stip, Military Academy "General Mihailo Apostolski", Skopje, North Macedonia
e-mail: aleksandar.petrovski@ugd.edu.mk
****Goce Delcev University' Stip, Military Academy "General Mihailo Apostolski", Skopje, North Macedonia
e-mail: rexhepmustafovski@gmail.com

Abstract

This paper explores the tactical employment of the Anti-Tank Guided Missile (ATGM) platoon in defensive operations, focusing on its effectiveness against armoured and mechanized threats in both conventional and hybrid warfare environments. Drawing on doctrinal frameworks such as FM 3-21.91, FM 71-1, and MCRP 3-30.7, the research evaluates key aspects including terrain-based siting, force distribution, survivability through mobility and camouflage, and synchronization with indirect fire and reconnaissance assets. Through simulated defensive scenarios, the study demonstrates that ATGM units deployed in decentralized, terrain-masked positions with overlapping fields of fire and ISR integration significantly improve engagement success and reduce vulnerability to counterattack. The findings suggest doctrinal and organizational refinements, such as the incorporation of hunter-killer tactics and loitering munitions at the platoon level, to meet the demands of multi-domain operations and support Force Design 2030 concepts. The paper concludes with practical recommendations for training, force structure adaptation, and integrated fires coordination.

Keywords:

Anti-Tank Guided Missile (ATGM) Platoon; Defensive Operations; Tactical Employment; Terrain Masking and Camouflage; Hunter-Killer Tactics; Combined Arms Integration.

Article info
Received: 30 May 2025; Revised: 27 June 2025; Accepted: 30 July 2025; Available online: 6 October 2025

Citation: Radovanovic, M., M. Zivkovic, A. Petrovski, and R. Mustafovski. 2025. "Doctrinal and Tactical Aspects of Deploying Anti-Tank Guided Missile Platoons in Defence." *Bulletin of "Carol I" National Defence University*, 14(3): 59-78. https://doi.org/10.53477/2284-9378-25-36

The tactical employment of the Anti-Tank Guided Missile (ATGM) (Radovanovic, et al. 2023b) platoon plays a vital role in modern defensive operations. As military engagements increasingly involve mechanized and armored threats supported by advanced mobility and firepower, the ability of defensive forces to neutralize such threats before they breach the defensive line is a mission-critical requirement. Recent armed conflicts, particularly the ongoing war in Ukraine, have demonstrated that Anti-Tank Guided Missile (ATGM) platoons achieve their greatest operational impact when deployed within a broader hybrid warfare framework. This approach integrates conventional maneuver elements with capabilities such as unmanned aerial reconnaissance, electronic warfare, precision artillery fire, and the use of camouflage and deception to disrupt enemy detection and targeting. Lessons from Ukraine have highlighted the importance of rapid relocation, effective concealment, and coordination between ATGM units and other combat assets to maintain both lethality and survivability. These developments confirm that the defensive role of ATGM platoons cannot be assessed in isolation but must be examined in relation to the multi-domain character of contemporary operations. ATGM platoons serve as the backbone of anti-armour resistance and are expected to deliver accurate, timely, and sustained fire support against enemy armour formations. Their success is not only a function of their weapons systems but also of their doctrinal positioning, coordination, and tactical flexibility. The correct deployment of these units can delay or stop an armoured advance, protect high-value defensive positions, and support infantry units holding the line.

According to Field Manual 71-1, ATGM platoons must be carefully positioned to take advantage of terrain, create overlapping fields of fire, and maintain concealment from enemy observation and targeting systems (Headquarters, Department of the Army 1998). Field Manual 3-98 reinforces this by outlining the importance of reconnaissance and early detection of enemy movement to allow ATGM units time to prepare engagements (Headquarters, Department of the Army 2009). Doctrinal publications such as MCRP 3-30.7 and MCWP 3-15.2 further support the idea that well-prepared indirect fire and long-range assets such as ATGM platoons must be embedded into a coordinated fire control plan (Headquarters, United States Marine Corps 2000; 2005). The Anti-Armour Company-Platoon Manual defines the deployment of combat crews and squads under various conditions of combat operations (Federal Secretariat for National Defense 1985). Field Manual FM 7-91 (Headquarters, Department of the Army 2002a) provides a detailed development of the engagement area for the anti-armour platoon and company.

Modern defensive doctrine increasingly incorporates multi-domain elements, including surveillance from unmanned aerial vehicles, communication with Tactical Operations Centres, and integration with mortar and artillery support. The FY2025 weapons strategy documents highlight that current investments are focused on enhancing the lethality and survivability of such units through encrypted battlefield communication, digital fire control, and real-time situational awareness

(United States Department of Defense 2023a; 2023b). However, even as technology advances, the core of ATGM employment remains rooted in tactics. The Hunter-Killer Platoon model introduces modern tactical concepts in which missile teams work in tandem with reconnaissance drones and loitering munitions to increase engagement success and reduce exposure time (Marine Corps Association 2022).

FM 3-21.71 outlines the operational readiness and placement of light infantry and support units, stating that ATGM platoons must not only deliver firepower but also maintain mobility and re-engagement capability in dynamic threat environments (Headquarters, Department of the Army 2002b). ATP 3-20.15 explains that in defensive operations, ATGM sections are most effective when placed at terrain chokepoints, reverse slopes, or concealed ambush zones to allow for first-strike advantage and survivability after firing (Headquarters, Department of the Army 2004). Tactical manuals such as the ROTC SOP and the Infantry Tactical SOP emphasize the importance of integrated planning, fire distribution, and command synchronization to achieve unit-level coherence during anti-armour engagements (United States Army ROTC n.d.; United States Army Infantry School n.d.a). The Anti-Armour Company–Platoon Manual emphasizes the specific conditions for employing ATGM platoons in manoeuvre terrain, including rugged terrain, mountainous areas, winter conditions, nighttime operations, and coastal defence (Federal Secretariat for National Defense 1985).

The historical foundation for these practices is not new. The 1943 British Army training document on anti-tank platoons highlights many of the same principles still relevant today, including field placement, lateral dispersion, and coordinated fire from multiple angles (War Office, British Army 1943). These concepts have evolved with new technology but remain consistent in their tactical value. Modern SOPs such as the ROTC-AC-TACSOP provide procedural detail on how platoon leaders should control fire missions, maintain secure communication with higher command, and coordinate with supporting assets (United States Army Cadet Command n.d.). These efforts are amplified when supported by secure signal and fire coordination measures as outlined in the Infantry Training SOP and Field Manual 7-90 (Headquarters, Department of the Army 1990; United States Army Infantry School n.d.b). Field Manual 3-21.91 (FM 7-91) (Headquarters, Department of the Army 2002a) defines the deployment model of combat positions for the anti-armour company and anti-armour platoons depending on the type of operation and mission.

Despite technological advancements, tactical fundamentals continue to determine the effectiveness of ATGM platoons. Whether operating in static defence, ambush configuration, or mobile blocking positions, their ability to achieve fire dominance over armoured threats depends on doctrine-driven decision-making, knowledge of terrain, and effective coordination with other elements. This paper focuses on evaluating the tactical deployment of the ATGM platoon in defensive scenarios by comparing several doctrinally supported configurations under simulated battlefield

conditions. These include linear forward-facing defence, flanking ambush positions, and layered depth-based defences. Each model will be assessed for its effectiveness in engagement success, survivability, and support coordination. By grounding the analysis in existing doctrine and validating it through simulation, this research aims to contribute practical insights for optimizing ATGM platoon employment in defensive operations.

Research Objectives and Hypotheses

The main objective of this study is to evaluate the effectiveness of three doctrinally recognized ATGM platoon deployment procedures in defensive operations, considering both conventional and hybrid warfare contexts. Specific objectives include:

1. To compare the operational performance of linear, echeloned, and dispersed defensive procedures using defined tactical indicators.
2. To identify the operational conditions under which each procedure provides maximum coverage, survivability, and adaptability.

Based on doctrinal understanding and observed field practices, the following hypotheses are formulated:

H1: The echeloned defense procedure provides superior coverage and survivability compared to linear and dispersed deployments under hybrid warfare conditions.

H2: The integration of reconnaissance data and coordinated fires significantly improves the overall effectiveness of ATGM platoon defense, regardless of the specific deployment procedure.

Literature Review

The tactical employment of Anti-Tank Guided Missile (ATGM) platoons in defensive operations is a critical element of modern combined arms doctrine. Over the decades, military field manuals and training documents have established a robust framework for understanding how these specialized units should be positioned, supported, and coordinated during operations involving enemy armoured formations. This section reviews seventeen doctrinal and strategic sources that collectively shape the theoretical and practical knowledge surrounding the deployment of ATGM platoons.

Doctrinal Foundations of ATGM Platoon Defence

Field Manual 71-1 provides one of the clearest tactical overviews of how company-level units, including ATGM platoons, should be deployed during mechanized defence operations. It emphasizes the importance of force protection, standoff range, concealment, and synchronized fields of fire that ensure early engagement and reduced risk of detection (Headquarters, Department of the Army 1998). Field Manual 3-98 complements this by offering detailed doctrine on reconnaissance integration and the role of early warning in anti-armour tactics. The document highlights how ATGM platoons should not operate in isolation but must work in coordination with surveillance elements and command structures (Headquarters, Department of the Army 2009).

ATP 3-20.15 is the most specialized reference focusing directly on anti-armour and ATGM platoon tactics. It explains how commanders should position these units using natural cover, concealment, reverse slope defence, and engagement from unexpected angles. It introduces the concept of mutual support between sections and emphasizes the value of terrain analysis in maximizing effectiveness (Headquarters, Department of the Army 2004). Field Manual 3-21.71 builds on this by describing defensive strongpoints and light infantry configurations, in which ATGM assets are layered within defensive belts to create depth and flexibility in response to enemy movement (Headquarters, Department of the Army 2002).
The British Army's 1943 Infantry Training Part VI on anti-tank platoons remains historically significant. Although the equipment described is outdated, the manual reinforces many tactical principles still applicable today. It discusses ambush from defilade, pre-registration of firing points, lateral dispersion, and the importance of interlocking fire zones, all of which are doctrinally echoed in modern NATO practices (War Office, British Army 1943).

Tactical Positioning and Defensive Configurations
MCRP 3-30.7 and MCWP 3-15.2, both developed by the United States Marine Corps, address the integration of ATGM platoons with infantry and indirect fire elements. These manuals discuss positioning options, the use of observation points, and fire planning in coordination with company and battalion-level headquarters (Headquarters, United States Marine Corps 2000; 2005). They highlight that terrain masking, line of sight control, and mobility are essential not only for successful engagement but also for post-shot survivability.

The Hunter-Killer Platoon concept introduces a more modern interpretation of ATGM operations. It proposes a hybrid model that combines traditional missile teams with mobile reconnaissance and loitering munitions. While this concept is still evolving, it supports the idea that ATGM platoons benefit greatly from real-time intelligence and dispersed ambush strategies. The platoon is no longer a static element but rather part of a dynamic targeting team that shifts position based on enemy movement and terrain advantage (Marine Corps Association 2022).

Modern tactics emphasize the importance of decentralization and flexibility. This is evident in the ROTC Tactical SOP and Infantry-TACSOP documents. These training guides instruct junior officers and non-commissioned leaders on how to organize ATGM units within patrol bases, fire teams, and ambush groups during field operations. They reinforce that anti-armour operations must be adaptable, with multiple fallback positions and communication lines to coordinate with supporting elements (United States Army ROTC n.d.; United States Army Infantry School n.d.a).

Supporting Elements: ISR, Mortars, and Command Coordination
While the core focus of defensive ATGM tactics is on fire and manoeuvre, modern doctrine recognizes that support from other elements can significantly enhance

performance. ATP 3-21.90 and MCWP 3-15.2 describe how mortars and indirect fire teams are used to suppress or channel enemy armour into the kill zones of ATGM platoons. Mortar units can also provide screening fire during ATGM platoon relocation, enhancing survivability (Headquarters, United States Marine Corps 2005; Headquarters, Department of the Army 1990).

FM 3-98 and the ROTC-AC-TACSOP highlight the importance of communication and command integration during anti-armour engagements. Real-time updates from reconnaissance units or unmanned aerial vehicles allow ATGM platoons to adjust their firing positions and time their engagement to exploit the enemy's vulnerability. These documents stress that while technology assists with targeting and synchronization, the tactical decision of when and where to strike remains a human command function (Headquarters, Department of the Army 2009; United States Army Cadet Command n.d.).

Strategic sources such as the FY2025 Defence Acquisition Reports identify ongoing investment in secure communication networks, battlefield sensors, and improved missile systems. These reports support the doctrinal shift toward precision engagement using integrated command and control, which directly impacts how ATGM platoons are expected to operate in future conflicts (United States Department of Defense 2023a; 2023b).

TABLE NO. 1

Summary of Key Contributions from Reviewed Literature

Ref	Title	Main Contribution
Headquarters, Department of the Army, 1998	FM 71-1	Explains ATGM roles in mechanized defensive operations
Headquarters, Department of the Army, 2009	FM 3-98	Outlines the integration of reconnaissance and ATGM employment
Headquarters, United States Marine Corps, 2000	MCRP 3-30.7	Tactical coordination of missile teams with maneuver and observation units
Headquarters, United States Marine Corps, 2005	MCWP 3-15.2	Describes supporting fire integration and battlefield positioning
United States Department of Defense, 2023a	FY2025 Weapons Report (1)	Strategic funding for missile, communication, and ISR systems
United States Department of Defense, 2023b,	FY2025 Weapons Report (2)	Focus on satellite and secure network support for tactical operations
United States Marine Corps, 2022	Hunter-Killer Platoon	Introduces modern flexible deployment and ISR-based targeting
Headquarters, Department of the Army, 2002	FM 3-21.71	Light infantry and ATGM integration in defensive strongpoints
Headquarters, Department of the Army, 2004	ATP 3-20.15	Specific doctrinal guidance on ATGM section placement and tactics
United States Army ROTC (n.d.)	ROTC SOP	Describes field-level ATGM fire control and team organization
United States Army Infantry School (n.d.)	Infantry-TACSOP	Tactical leadership procedures for ambush and fire distribution planning
War Office, British Army, 1943	1943 Anti-Tank Platoon Manual	Historical basis for ambush, flanking, and interlocking fire planning
United States Army Cadet Command (n.d.)	ROTC-AC-TACSOP	Coordination of ATGM platoons with command and signal planning
Headquarters, Department of the Army, 1990	ATP 3-21.90	Indirect fire coordination and support of anti-armor elements
Headquarters, Department of the Army, 2002	FM 3-21.91 (FM 7-91)	Tactical Employment of Antiarmor Platoons and Companies
United States Army Infantry School (n.d.)b	Infantry Training SOP	Fire control, defensive positioning, and coordination between platoon-level units
Federal Secretariat for National Defense, 1985	*Anti-Armour Company–Platoon Manual*	Conduct of anti-armor operations under varying weather and terrain conditions

The table summarizes the central contributions of all fifteen references reviewed in this study. Each document supports a different aspect of the doctrinal, operational, or strategic understanding of how ATGM platoons are employed in defensive engagements. These sources collectively serve as the foundation for the simulated scenarios, tactical analysis, and doctrinal comparisons presented in the following sections of this paper.

Methodology

This study uses a multi-phase methodology to evaluate the tactical effectiveness of the Anti-Tank Guided Missile (ATGM) platoon in defensive operations. The approach integrates doctrinal analysis, simulation modelling, and comparative evaluation of battlefield performance under varying tactical conditions. All tactical models are grounded in military doctrinal publications and reflect realistic field scenarios extracted from seventeen validated sources.

Doctrinal Analysis of ATGM Platoon Employment

The first phase involved a comprehensive review of U.S. Army and Marine Corps field manuals and training publications related to the organization, capabilities, and employment of anti-tank platoons. Manuals such as FM 3-21.71, FM 3-21.91, and ATP 3-20.15 provide detailed guidelines on platoon composition, firing post selection, ambush planning, terrain exploitation, and integration with infantry and reconnaissance units (Headquarters, Department of the Army 2002; 2004). FM 71-1 and the 1943 British Anti-Tank Platoon manual were reviewed for insights on historical and mechanized deployment of anti-armour teams in layered defence strategies (Headquarters, Department of the Army 1998; War Office, British Army 1943).

From these documents, key doctrinal factors were extracted:

- Preferred firing range and standoff distances;
- Use of enfilade and defilade positioning;
- Mobility and shoot-and-scoot doctrine;
- Force distribution across linear, flanking, and depth-based layouts;
- Integration with indirect fire support and ISR platforms (Radovanovic, et. al. 2023a).

This doctrinal foundation guided the design of simulation scenarios and the performance metrics selected for analysis.

Tactical Scenario and Threat Definition

In the second phase, a reference battlefield scenario was constructed to model a defensive engagement between a friendly ATGM platoon and an enemy mechanized company. The environment is set in a semi-open, hilly terrain with intermittent vegetation and two key approach avenues. The enemy force consists of ten main battle tanks and supporting infantry fighting vehicles approaching from multiple angles.

The friendly force consists of a fully equipped ATGM platoon with six launchers organized into two firing sections. The platoon has access to UAV-generated ISR data, mortar support, and real-time position tracking via secured communication with the Tactical Operations Centre. However, the communication layer is treated as a supporting element, not the primary research focus.

Three tactical configurations are tested:

1. Linear frontal deployment across a ridge with overlapping fields of fire;
2. Ambush flanking setup with split sections covering separate engagement zones;
3. Depth-based echelon defence using fallback positions and mobility.

Each configuration is evaluated for engagement success, platoon survivability, and tactical delay imposed on enemy advancement.

Anti-Tank Guided Missile (ATGM) Platoon Deployment Model

Based on the analysis of various military manuals, several models for the deployment of an anti-armour platoon in defensive operations have been developed. These models are closely aligned with the disposition and strength of enemy forces and allow for further adaptation and refinement depending on the specifics of the tactical situation. The flexibility of these deployment frameworks enables commanders to optimize the positioning of anti-armour assets to effectively counter anticipated threats and terrain conditions, thus enhancing the unit's overall operational effectiveness in the defence.

The organizational structure of an ATGM platoon varies based on national military doctrine, the specific ATGM system employed, and whether the unit operates as part of a mechanized, motorized, or dismounted infantry force. Despite these variations, an ATGM platoon typically comprises 2 to 3 ATGM sections, each containing 2 to 3 firing teams. This analysis focuses on the tactical employment of an ATGM platoon organized into three sections, a configuration that enhances tactical flexibility and enables more effective allocation of anti-armor fires in defensive operations.

The tactical formation of an anti-armour platoon in a column (Figure 1) configuration involves the sequential placement of vehicles or squads, where each element maintains a distance of approximately 100 to 200 meters from the next. This formation is frequently employed in urban environments and mountainous terrain, particularly in areas with significant elevation differences. Under such conditions, where visibility is limited, ambushes are likely, and manoeuvrability is constrained, the increased spacing between elements reduces the risk of a single enemy attack affecting the entire unit. In urban settings, this formation enables improved coverage of intersections and street approaches, as well as a more rapid and flexible response to threats emerging from multiple directions, including ambushes. In mountainous or high-relief environments, where terrain restricts both movement and line of sight, the spacing enhances control over elevation-dominant routes and enables

manoeuvrings from protected positions. Additionally, this configuration facilitates the use of natural cover and concealment and supports the effective organization of fire support. Moreover, the column formation contributes to improved flank and rear security, as it allows for enhanced observation and more agile repositioning in the event of enemy contact. This setup supports sustained situational awareness and increases the survivability of anti-armour elements in complex operational environments.

The line formation of an anti-armour platoon (Figure 2) entails the lateral deployment of squads in a linear array along the forward line of own troops (FLOT), with intervals of 100 to 150 meters between elements. This configuration is typically employed in wide-area coverage scenarios, particularly on manoeuvrable terrain, in prepared defensive positions, or during delaying (elastic) defence involving multiple successive primary, alternate, and supplementary positions in depth.

This tactical disposition provides several doctrinally recognized advantages:

- Overlapping fields of fire, ensuring maximum coverage and mutual support between weapon systems in accordance with direct fire planning principles;
- Improved early target acquisition and engagement capabilities against armoured threats;
- Flexible fire planning, especially when employing mixed anti-armour assets;
- Reduced vulnerability to enemy indirect fire or air-delivered munitions, due to increased dispersion and decentralized target signature.

The 100–150 meter interval is optimized to maintain C3 (command, control, and communication) effectiveness, ensure line-of-sight (LOS) where feasible, and facilitate fire and manoeuvre while preserving the tactical autonomy of each squad under degraded conditions. In anticipation of an enemy armoured counterattack or breakthrough, the line formation enables saturated direct fire coverage across the axis of approach, while preserving the ability to conduct manoeuvre in depth — including fighting withdrawal, lateral repositioning, or flanking engagement.

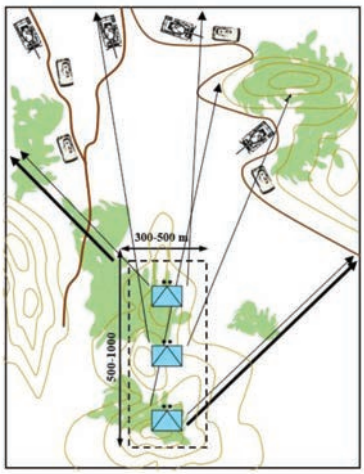

Figure 1 ATGM Platoon in Column

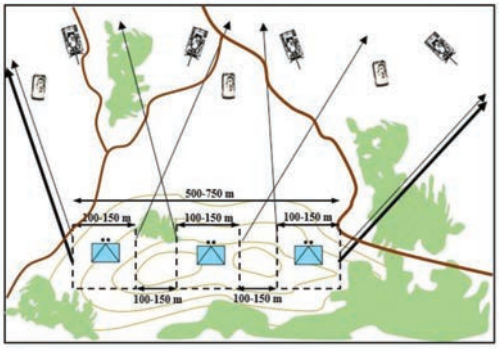

Figure 2 ATGM Platoon in Line

The anti-armour platoon formation in a reverse wedge (also known as a "backward wedge") (Figure 3) is employed to achieve enhanced flexibility and protection in combat situations against armoured threats. In this formation, individual anti-armour missile launchers or firing units are arranged to form an angle oriented backward, with the apex of the wedge facing the platoon's rear.

Advantages and Reasons for Employment:

- This formation enables control of the space behind the leading combat elements, which is critical for defence against surprise armoured or infantry attacks from the rear.
- The reverse wedge allows rapid reaction by anti-armour units to potential threats approaching from lateral or rear sectors, thereby reducing the risk of unexpected flanking attacks.
- Thanks to the angular arrangement, units can easily reposition and redeploy without complex realignments. This is particularly beneficial in dynamic and unpredictable combat environments.
- Anti-armour systems deployed in this formation can cover a wider area with fires from multiple directions, increasing the probability of detecting and neutralizing enemy armoured targets.

Limitations:

- Potentially reduced forward concentrated firepower compared to a traditional forward wedge formation.
- Requires effective communication and coordination among individual anti-armour assets to maintain formation integrity and operational effectiveness.

The anti-armour platoon formation in a forward wedge is employed to maximize offensive firepower concentration and direct engagement of armoured targets (Figure 4). In this formation, individual anti-armour missile launchers or firing units are arranged to form an angle oriented forward, with the apex of the wedge facing the enemy.

Advantages and Reasons for Employment:

- This formation allows the platoon to deliver a highly focused and coordinated volume of fire directly towards the enemy's front, increasing the effectiveness of anti-armour engagements.
- The forward wedge facilitates rapid target acquisition and engagement, enabling swift suppression or destruction of approaching armoured threats.
- The arrangement supports clear lines of sight and communication between units, facilitating synchronized manoeuvres and fire coordination.
- The forward wedge can be easily adapted to terrain features, allowing the platoon to exploit natural cover and concealment while maintaining an offensive posture.

Limitations:

- Reduced coverage of rear and flanking sectors, potentially exposing the platoon to attacks from the sides or rear.
- Less flexibility in repositioning without breaking the formation, which can be disadvantageous in rapidly changing combat situations.

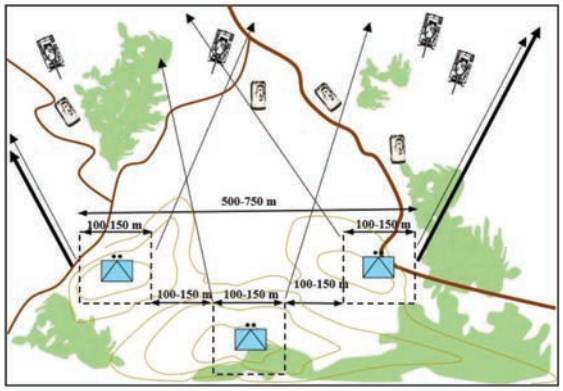

Figure 3 ATGM Platoon backward wedge

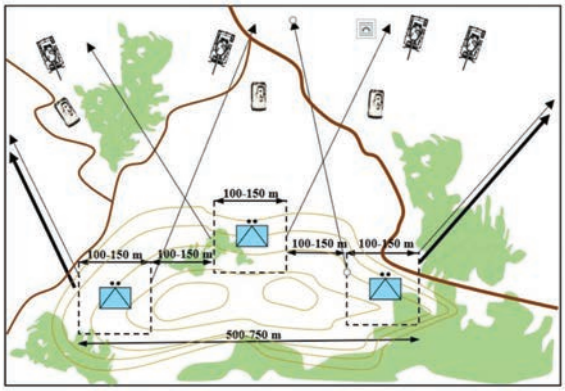

Figure 4 ATGM Platoon forward wedge

In the "Echelon Left I" formation, two squads on the left flank are positioned behind the right-flank squad at a distance of approximately 150 to 200 meters (Figure 5). This deployment provides combined depth protection and enhanced tactical flexibility during combat operations.

Detailed Tactical Advantages:

- Positioning the left-flank squads rearward of the right-flank unit ensures effective control of the area behind the primary forward line. This arrangement is critical for countering enemy flanking manoeuvres and surprise attacks originating from the rear sector. The left flank elements maintain surveillance over enemy movements and enable a timely response to any bypass attempts.
- The 150 to 200 meter lateral and rearward spacing provides sufficient room for rapid repositioning and adjustment of unit positions without compromising the integrity of the overall formation. This flexibility is especially advantageous in complex operational environments such as urban or wooded terrain.
- Maintaining this spacing preserves line-of-sight and communication links between units, reducing the risk of physical interference or movement path conflicts. This facilitates effective command and control throughout the formation.
- The rearward placement of left flank squads acts as a force multiplier by providing a protective anchor and enabling rapid reaction to flanking threats, thus increasing the overall resilience of the formation.

Potential Limitations:

- Due to the positional offset, left flank squads may experience a marginal delay in responding to immediate threats directed at the right flank or main battle line.
- Successful employment of this formation necessitates clear command directives and robust communications systems to maintain situational

awareness and formation cohesion.

- In high-tempo combat scenarios, the physical separation between squads may contribute to delayed transmission and reception of critical tactical information.

The **"Echelon Left II" formation** of an anti-tank squad represents a tactical deployment in which each successive squad is positioned to the left and to the rear of the preceding one. In Figure 6, it is clearly shown that the right-flank squad is deployed forward and acts as the lead element, while the remaining two squads on the left flank are echeloned in depth, with an approximate interval of 150 to 200 meters diagonally to the left and rear.

This type of formation is particularly suitable when it is anticipated that the main thrust of enemy armoured and mechanized forces will occur frontally or from the right. The "Echelon Left" formation enhances both survivability and manoeuvrability of the unit. Echeloning the squads in depth reduces the probability of multiple elements being simultaneously affected by enemy artillery or air strikes. At the same time, such a disposition facilitates better utilization of terrain and available cover, and enables easier execution of redeployment, counterattack manoeuvres, or withdrawal in case of an unfavourable tactical situation. Command and control are simplified, as all elements remain within visual and radio communication range, allowing effective coordination and timely transmission of orders.

Essentially, the "Echelon Left II" formation is employed when it is necessary to establish a flexible anti-tank defence, provide flanking fire from the left, and reduce the risk of concentrated combat losses due to a frontal assault. Its implementation requires well-trained crews, efficient communication, and clearly defined positions for each squad relative to the unit's main axis of engagement.

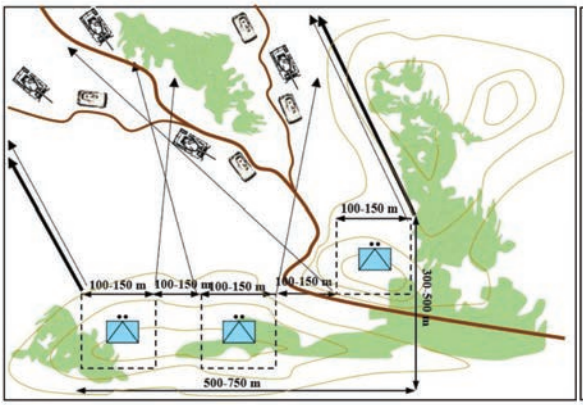

Figure 5 ATGM Platoon Echelon Left I

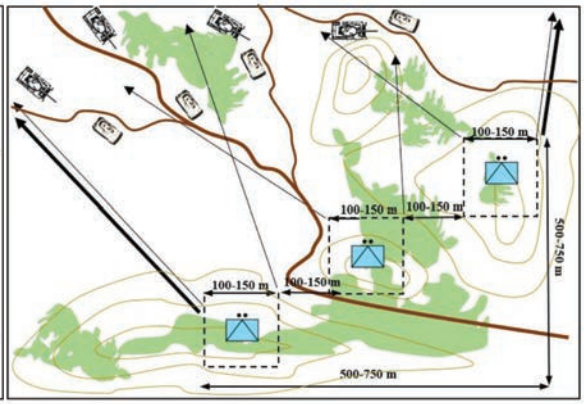

Figure 6 ATGM Platoon Echelon Left II

The **"Echelon Left III" formation** of the anti-tank platoon, shown in *Figure 7*, features a tactical layout in which the right-flank and centre squads are deployed on the same line, while the left-flank squad is echeloned to the rear and left at a distance of approximately 150–200 meters. The entire formation covers a frontage of approximately 500 to 750 meters.

This configuration allows for flanking fire from the left, while maintaining the forward firepower of the main elements along the likely enemy axis of advance. The centre and right-flank squads provide direct frontal engagement, while the rear-positioned left squad offers flexibility for engaging targets from oblique angles, executing manoeuvres, or forming a secondary line of fire.

The depth and dispersion of the formation enhance the platoon's survivability against concentrated enemy fires (e.g., artillery, air strikes), while still enabling effective command and control through both line-of-sight and radio communications. The formation is particularly suited for scenarios involving expected frontal or right-flank enemy movement, offering improved fire distribution and tactical adaptability.

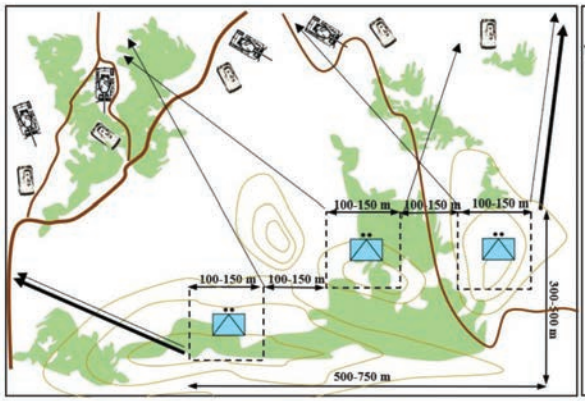

Figure 7 ATGM Platoon Echelon Left III

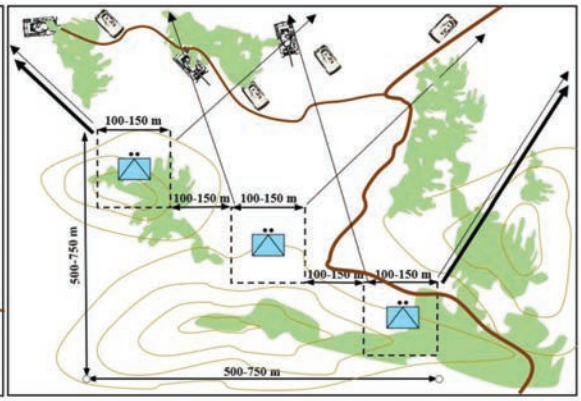

Figure 8 ATGM Platoon Echelon Right I

The **"Echelon Right"** formation (I, II, and III) possesses the same tactical and technical characteristics as the left echelon formation, with the difference that the unit arrangement is mirrored to the right side (Figures 8, 9, and 10). In other words, the layout of elements and their positions remain identical but are symmetrically positioned relative to the formation's central axis.

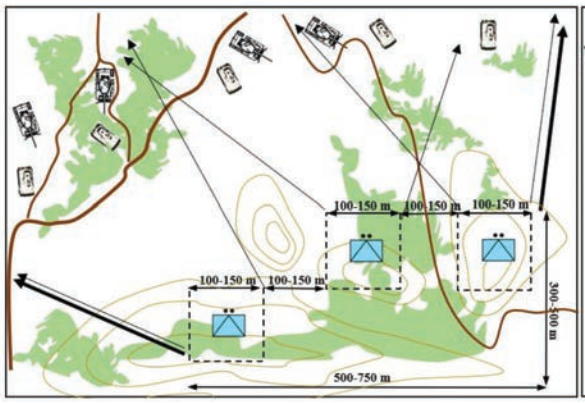

Figure 9 ATGM Platoon Echelon Right II

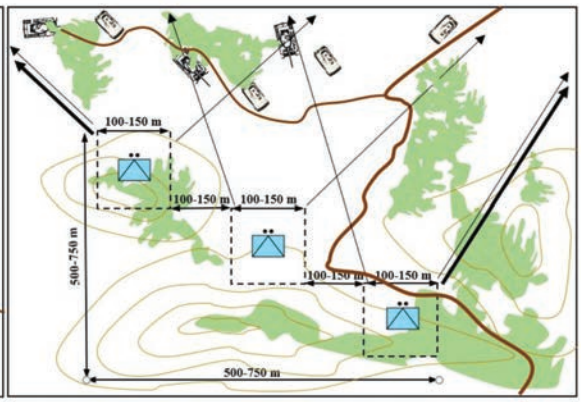

Figure 10 ATGM Platoon Echelon Right III

Simulation Environment and Execution

To evaluate the ATGM platoon's performance under each configuration, a series of simulations was conducted using a MATLAB-based modelling environment. The terrain was modelled using elevation data and vegetation density layers. Enemy

movement was randomized within doctrinally accurate approach routes. Sensor detection, engagement delay, and missile hit probability were calibrated based on doctrinal specifications outlined in ATP 3-20.15 and FM 3-21.91 (Headquarters, Department of the Army 2002; 2004).

Each scenario ran ten times to account for variability in detection time, targeting delay, and enemy manoeuvres. Metrics recorded include:

- Number of enemy vehicles destroyed;
- Time to first engagement;
- Average missile-to-hit delay;
- Platoon survival rate at mission end;
- Total mission time until enemy breakthrough or halt.

Data from these simulations is used to compare which configuration offers the most favourable trade-off between firepower, concealment, and survivability.

Integration of ISR and Supporting Assets

Although the ATGM platoon is the primary focus of this study, integration with supporting elements such as UAVs, mortars, and TOC coordination is considered in simulation modelling. UAVs are modelled as ISR assets that reduce detection time and enhance firing readiness. Mortar support is used to simulate enemy suppression and area denial during platoon relocation. Communication systems are assumed to function as described in MCRP 3-30.7 and FM 3-98, ensuring situational awareness between the platoon and command elements (Headquarters, Department of the Army 2009; Headquarters, United States Marine Corps 2000).

These support tools are evaluated for their tactical impact on decision-making speed and platoon repositioning efficiency, not for their technical performance.

Results and Tactical Effectiveness Analysis

This section presents the simulation results evaluating the tactical performance of the Anti-Tank Guided Missile (ATGM) platoon in three doctrinally informed defensive configurations: Linear Deployment, Flanking Ambush, and Depth-based Defence. The analysis draws from multiple scenarios runs and performance metrics that reflect key tactical outcomes, including engagement success, platoon survivability, and overall delay imposed on the enemy advance. Each configuration was tested ten times under consistent battlefield conditions, and averages were calculated for comparative evaluation.

Engagement Effectiveness: Enemy Vehicles Destroyed

As shown in Figure 11, the Flanking Ambush configuration resulted in the highest number of enemy armoured vehicles neutralized, with an average of 8 kills per scenario. This configuration allowed ATGM teams to engage from lateral or rearward positions, exploiting side and rear armour vulnerabilities of advancing enemy tanks. The ability to remain undetected until the first engagement provided a critical advantage in achieving high-impact first strikes.

The Depth-based Defence achieved 6 vehicle kills, demonstrating effective use of echeloned firing positions that allowed the platoon to conduct successive engagements while maintaining cover and manoeuvre options. The Linear Deployment, while doctrinally simpler to organize, resulted in only 5 kills, as its frontal exposure made ATGM positions more susceptible to early detection and return fire.

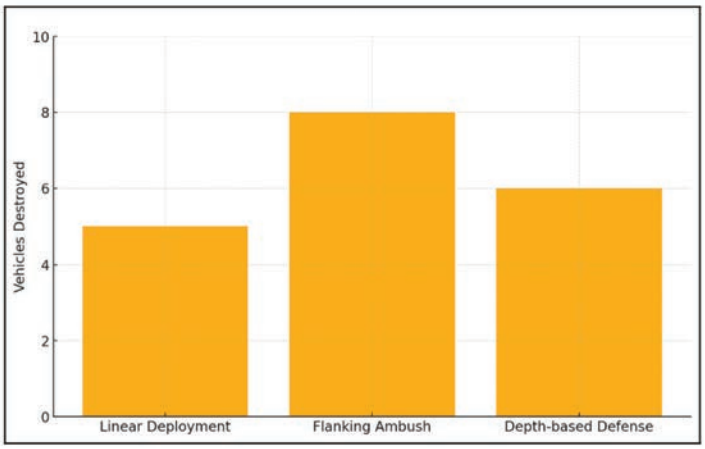

Figure 11 Number of Enemy Vehicles Destroyed by Configuration

The Flanking Ambush configuration achieved the highest success, destroying an average of 8 enemy vehicles per scenario. The Depth-based Defence model achieved 6 kills, benefiting from delayed engagement and tactical repositioning. The Linear Deployment was least effective, with 5 vehicles destroyed, likely due to early detection and higher vulnerability. This metric confirms doctrinal principles found in ATP 3-20.15 and FM 3-21.91, which emphasize ambush and terrain exploitation as key to effective anti-armour tactics (Headquarters, Department of the Army 2002; 2004).

Platoon Survivability under Fire

Platoon survival rate is a critical indicator of tactical success. As seen in Figure 12, the Flanking Ambush achieved the highest survivability at 70%, benefiting from concealment, terrain masking, and minimal early exposure. This model allowed firing teams to displace rapidly after launching missiles, in line with the shoot-and-move doctrine.

The Depth-based Defence maintained a respectable 60% survival rate, as the fallback structure gave each section time to fire and relocate without concentrated return fire. The Linear Deployment, by contrast, experienced heavy attrition with a survival rate of just 40%. In this configuration, multiple positions were exposed simultaneously, increasing the platoon's vulnerability to suppression or direct hits from enemy support elements.

The Flanking Ambush again performed best, with a 70% survival rate, attributed to concealed positions and limited exposure. The Depth-based Defence provided

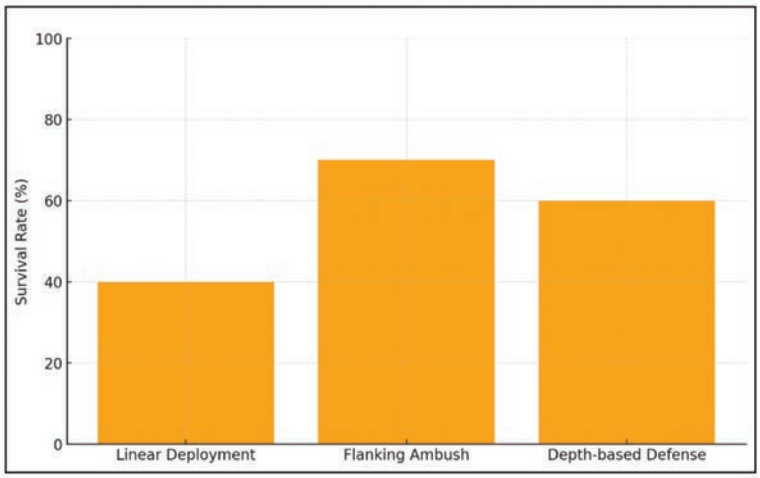

Figure 12 ATGM Platoon Survival Rate by Configuration

moderate survivability at 60%, leveraging mobility and terrain for fallback. The Linear Deployment saw the lowest survival rate at 40%, with units often exposed early and receiving return fire. These results reinforce the importance of distributed positioning and delayed detection emphasized in FM 71-1 and MCRP 3-30.7 (Headquarters, Department of the Army 1998; Headquarters, United States Marine Corps 2000).

Delay of Enemy Advance: Time to Halt

The ability of an ATGM platoon to delay enemy manoeuvre provides critical time for repositioning, reinforcement, and coordination with higher command. Figure 13 illustrates that Flanking Ambush created the longest delay, halting enemy movement for an average of 18 minutes. This delay was the result of sudden, coordinated fire from unexpected angles that forced the enemy into disorganized manoeuvre and regrouping.

The Depth-based Defence caused a 15-minute delay, effectively staggering the engagement timeline and forcing enemy units into incremental exposure. Linear Deployment achieved only a 12-minute delay, as the predictable engagement zone allowed the enemy to rapidly suppress and bypass ATGM firing positions.

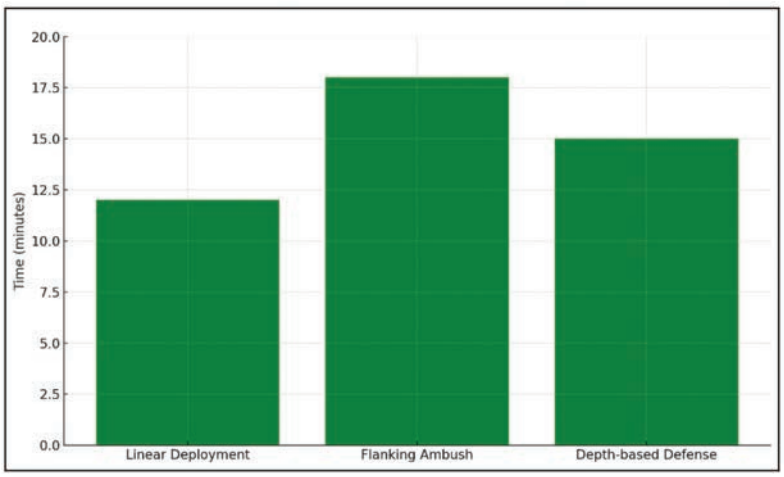

Figure 13 Time to Enemy Halt by Configuration

The Flanking Ambush configuration delayed the enemy advance by an average of 18 minutes, allowing more time for support to reposition. The Depth-based Defence caused a 15-minute delay, effective in layered attrition. The Linear Deployment achieved a shorter delay of 12 minutes, as the enemy was able to identify and suppress ATGM positions earlier. This outcome highlights the tactical advantage of surprise and channelling enemy movement into constrained kill zones, consistent with the principles outlined in FM 3-98 and the Infantry-TACSOP (Headquarters, Department of the Army 2009; United States Army Infantry School n.d.a).

The simulation results clearly show that Flanking Ambush tactics provide the most effective balance between firepower and survivability in defensive operations. These results align with doctrinal guidance from ATP 3-20.15 and FM 3-21.91, which recommend enfilade fire, terrain masking, and decentralized positioning for anti-armour units. The Depth-based Defence also performed well and offers value in complex terrain where manoeuvre space allows fallback. In contrast, Linear Deployment should be avoided in open terrain unless heavily reinforced or concealed. These results validate the importance of terrain exploitation, lateral dispersion, and integrated ISR support when tactically employing ATGM platoons.

Doctrinal Implications and Tactical Insights

The results of the simulation clearly validate that the Flanking Ambush configuration offers the most favourable trade-off between lethality and survivability. The performance gains are attributed to its alignment with classical ambush doctrine, tactical concealment, and enfilade fire geometry. This configuration also leverages ISR integration most effectively, as UAV reconnaissance feeds were used to coordinate positioning and timing without direct visual contact.

The Depth-based Defence performed well in scenarios where fallback and terrain manoeuvre were available, making it suitable for delaying actions and rear-guard operations. While not as lethal as flanking ambushes, it provides sustained fire capacity with greater survivability than linear setups.

The Linear Deployment remains the least effective in open or semi-open terrain without support from suppressive fire or concealment measures. Its frontal geometry often exposed multiple sections at once, increasing vulnerability and limiting tactical flexibility. However, it may still be appropriate in static defence of critical chokepoints where terrain prohibits flanking movement.

Conclusion

The tactical employment of the Anti-Tank Guided Missile (ATGM) platoon in defensive operations remains a decisive element in modern warfare, particularly when confronting armoured and mechanized threats. This research evaluated doctrinal principles, historical guidance, and simulation-based performance across three distinct

deployment configurations: linear frontal defence, flanking ambush, and depth-based echelon defence. The results clearly indicate that flanking ambush tactics offer the most favourable balance of lethality, survivability, and operational impact.

The simulation results demonstrated that the flanking ambush configuration not only achieved the highest number of enemy vehicle kills but also maintained the highest platoon survival rate and imposed the longest delay on enemy advancement. These outcomes validate key doctrinal concepts outlined in FM 3-21.91 and ATP 3-20.15, particularly regarding the importance of terrain exploitation, concealment, and fire from unexpected angles. The depth-based defence configuration also performed well and may serve effectively in situations requiring flexible repositioning and sustained attrition. Conversely, linear deployment proved to be the least effective model in open terrain, exposing ATGM teams to early detection and concentrated enemy fire.

While supporting elements such as unmanned aerial vehicles, indirect fire support, and secure communications contributed to operational awareness and coordination, the core determinant of ATGM effectiveness remained the tactical configuration and its alignment with battlefield terrain and enemy movement. These findings reinforce the importance of doctrinally informed planning, continuous terrain analysis, and decentralized decision-making at the platoon level.

While the comparative results of the three evaluated procedures show consistent patterns, the study is limited by the scope of scenarios considered and the selected simulation parameters. The procedures were tested under controlled conditions that may not fully reflect the complexity and variability of real combat environments. Future research should expand the analysis by including additional tactical procedures, more diverse terrain types, and variable threat profiles to capture a broader operational spectrum. This extended approach would enable a more conclusive assessment and provide deeper insights for operational planning and doctrinal refinement.

For commanders and planners, this study offers actionable insights. ATGM platoons should be employed in dispersed, terrain-masked positions with ISR-enabled targeting and fallback maneuver capability. Training programs should emphasize rapid position transitions, fire discipline under concealment, and coordination with reconnaissance assets. Future doctrinal updates should consider integrating modern hunter-killer concepts and loitering munitions to expand the role of ATGM platoons in multi-domain operations.

This paper confirms that when tactically employed with doctrinal precision and strategic foresight, the ATGM platoon is a force multiplier capable of decisively shaping the outcome of defensive engagements against armoured threats.

References

Federal Secretariat for National Defense. 1985. *Anti-Armour Company–Platoon Manual,* Belgrade, Serbia.

Headquarters, Department of the Army. 1998. *FM 71-1: Tank and Mechanized Infantry Company Team.* Washington, D.C., United States Army.

___. 2002a. *FM 3-21.91 (FM 7-91): Tactical Employment of Antiarmor Platoons and Companies Headquarters.* Washington, D.C., United States Army.

___. 2002b. *FM 3-21.71: Mechanized Infantry Platoon and Squad.* Washington, D.C., United States Army.

___. 2004. *ATP 3-20.15: Tank Platoon.* Washington, D.C., United States Army.

___. 2009. *FM 3-98: Reconnaissance and Security Operations.* Washington, D.C., United States Army.

___. 2019. *ATP 3-21.90: Tactical Employment of Mortars.* Department of the Army, United States.

Headquarters, United States Marine Corps. 2000. *MCRP 3-30.7: Commander's Tactical Handbook.* Quantico, Virginia, United States Marine Corps.

___. 2005. *MCWP 3-15.2: Tactical Employment of Mortars*, Quantico, Virginia, United States Marine Corps.

Marine Corps Association. 2022. *Implementation of the Hunter-Killer Platoon Concept*, Marine Corps Warfighting Laboratory, Quantico, Virginia.

Radovanović, Marko, Petrovski Aleksandar, Žnidaršič Vinko, and Behlić Aner. 2023a. "The C5ISR System Integrated with Unmanned Aircraft in the Large-Scale Combat Operations." *Vojenské rozhledy* 32(2): 098-118. https://doi.org/10.3849/2336-2995.32.2023.02.098-118

Radovanović, Marko, Petrovski Aleksandar, Smileski Saša and Jokić Željko. 2023b. "Analysis of the development of five generation of anti-armor missile systems." *Scientific Technical Review* 73(1): 26-37. https://doi.org/10.5937/str2301026R

United States Army Cadet Command. n.d. *ROTC-AC-TACSOP: Advanced Camp Tactical Standard Operating Procedures.* Fort Knox, Kentucky, United States Army.

United States Army Infantry School. n.d. a. *Infantry Tactical SOP.* Fort Benning, Georgia, United States Army.

___. n.d. b. *Infantry Training SOP*, Fort Benning, Georgia, United States Army.

United States Army ROTC. n.d. *ROTC Tactical SOP.* U.S. Army Cadet Command, Fort Knox, Kentucky.

United States Department of Defense. 2023a. *FY2025 Weapons Systems Report – Volume 1.* Office of the Under Secretary of Defense for Acquisition and Sustainment. Washington, D.C.

https://doi.org/10.53477/2284-9378-25-36

___. 2023b. *FY2025 Weapons Systems Report – Volume 2.* Office of the Under Secretary of Defense for Acquisition and Sustainment. Washington, D.C.

War Office, British Army. 1943. *Infantry Training Part VI: The Anti-Tank Platoon*. The War Office, London, United Kingdom.

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

Mainstreaming Global Goals: the Impact of SGD One on Poverty Reduction in Oyo and Osun States, Nigeria

Abdulrauf AMBALI*
Ibrahim O. SALAWU**
Habee A. SHEU***

*Professor, Department of Politics and Governance, Kwara State University, Malete
https://orcid.org/0009-0000-0723-3593
**Associate Professor, Department of Politics and Governance, Kwara State University, Malete
https://orcid.org/0009-0001-5393-294X
***Lecturer II, Emmanuel Alayande University of Education, Oyo
e-mail: ry1207@gmail.com
https://orcid.org/0000-0002-8825-7294

Abstract

This study evaluates the impact of Sustainable Development Goal One (SDG 1) on poverty reduction in Nigeria, with a specific focus on Oyo and Osun States. Despite numerous national poverty alleviation policies, including SDG-aligned initiatives such as the Conditional Cash Transfer (CCT), Government Enterprise and Empowerment Programme (GEEP), and Youth Employment and Social Support Operation (YESSO), poverty remains pervasive in both states. Using a descriptive household survey method with 397 household respondents, the study finds a statistically significant disconnect between the planning and implementation of SDG 1 programmes, particularly in employment generation and policy execution. Although awareness and participation levels are relatively even across programme types, effectiveness remains limited. Probit regression analysis reveals that among four intervention areas, Income Support, Service Access, Health Support, and Employment, only Service Access significantly affects poverty outcomes, and this effect is negative due to inadequate delivery mechanisms. The study concludes that structural and institutional challenges, weak coordination, poor data management, and limited monitoring capacity impede the transformative potential of SDG 1 in the two states. It recommends a shift from short-term palliative interventions to sustainable, data-driven, and community-inclusive strategies that prioritize service delivery, employment, and governance reform.

Keywords:
Poverty; Sustainable Development Goals (SDG); Poverty Reduction; Programme Service Access and Development Policy.

Article info
Received: 25 July 2025; Revised: 29 August 2025; Accepted: 10 September 2025; Available online: 6 October 2025

Citation: Ambali, A., I.O. Salawu, and H.A. Sheu. 2025. "Mainstreaming Global Goals: the Impact of SGD One on Poverty Reduction in Oyo and Osun States, Nigeria." *Bulletin of "Carol I" National Defence University*, 14(3): 79-100. https://doi.org/10.53477/2284-9378-25-37

Poverty remains one of the most persistent challenges to human development globally, and Nigeria is no exception. A majority of the world's population lives below the poverty line set by the World Bank. It signifies that a significant portion of the world population lives on an income of less than two United States dollars per day (Kharas and Dooley 2022). In many countries of the world, including the prosperous ones, there are significant signs of poverty with a vast percentage of people patchily clothed, underfed, badly housed, and lacking access to basic amenities of life.

At its core, poverty encompasses multifaceted dimensions, extending beyond mere financial constraints to encompass inadequate access to education, healthcare, and opportunities. The expression of poverty means the absence of income and productive resources, impoverished livelihoods, hunger, malnutrition, compromised health, restricted or no access to education and essential services, rising mortality from illnesses, homelessness, insufficient housing, unsafe living conditions, and social discrimination, including exclusion. The problem of poverty is, however, prominent in developing countries. A vast majority of the people in Africa and Asia are deemed impoverished and wretched. The bulk of the nations in these continents are Agrarian, with the majority of their people relying on agriculture, export of primary products, and related activities for a living. For the majority living in these continents, poverty is an endemic and devastating reality.

The number of people living in extreme poverty in Nigeria has increased from time immemorial. The 2022 Multidimensional Poverty Index (MPI) Survey by the National Bureau of Statistics (NBS) revealed that 63% of the Nigerian population, approximately 133 million people, is multidimensionally poor. With a national MPI value of 0.257, the data indicate that the average poor person experiences over one-quarter of the total possible deprivations (NBS 2022). The degree of progress made in reducing poverty remains the yardstick for evaluating the effectiveness of development interventions.

Nigeria has put in place development plans, policies, and programmes to fight poverty in Nigeria. Since independence, different policies have been utilized to tackle poverty in Nigeria. These encompassed the First to the Fifth National Development Plans, cost-of-living allowance, panels for wage review, Adebo and Udoji panels, and the 1981 National Minimum Wage Act. Other initiatives included Operation Feed the Nation, River Basin Development Authorities, Agricultural Development Programme, Agricultural Credit Guarantee Scheme, Rural Electrification Scheme, and Green Revolution (Olayide 1976; Ayida 1987; Ayo 1988; Anyanwu, et al. 1997; Ijaiya and Nuhu 2021). Various poverty alleviation programmes were introduced in the democratic period in Nigeria. These are the Poverty Alleviation Programme (PAP), which later changed to the National Poverty Eradication Programme (NAPEP). Also, the National Economic Empowerment and Development Strategy (NEEDS), Seven-Point Agenda, and Transformation Agenda. The following programmes have been implemented by Nigeria's Federal Government; the

Community Service, the Women and Youth Employment Scheme, the SURE-P, Economic Recovery and Growth Plan, and several social investment programmes including conditional cash transfers, NHGSFP, GEEP (trader money and market money) N-Power, infrastructure investment, business environment improvement, and digital growth promotion (Ogwumike 2001; Ibeanu 2004; Igbuzo 2004; NPC 2004; Ole 2009; Dodo 2010; FGN 2012, 2014; NSIO 2016; NASSCO 2020; Ijaiya and Nuhu 2011).

While some modest economic growth has been achieved, poverty has not been significantly reduced. The economic growth shows a considerable growth measured by real per capita GDP or national income, price stability, and reduced unemployment through the coordination of monetary and fiscal policies. However, access to fundamental necessities like food, healthcare, education, housing, clothing, transport, water, and sanitation to enhance the living standards of impoverished populations remains stagnant (Ogwumike 2001; Ijaiya and Nuhu 2011). The trickle-down effect of these programmes, policies, and strategies has not materialized, and the poor are not better off than they were previously.

In response to the approval of the 2030 Agenda, Nigeria immediately commenced the National Implementation of the SDGs at the National and Sub-national Levels. To promote the suitable implementation of the goal by establishing institutional mechanisms at the national and subnational levels. The initiation of the Sustainable Development Goals (SDGs) in 2015 was a defining moment in world efforts to deal with pressing social, economic, and environmental issues. Nigeria is committed to the Sustainable Development Goals (SDGs). Through the Osun and Oyo governments, it has made regional commitments to implement SDG-related initiatives and programmes aimed at eradicating poverty and enhancing the well-being of the people. Poor people are in significant numbers in both States, and there are a lot of socio-economic problems. SDG programme and policies are essential for help. Under the SDGs, the states mainstreamed and developed a number of poverty reduction schemes and initiatives. These include the establishment of the Oyo State Youth Entrepreneurship in Agriculture Programme, OYYEAP, which trains and provides assistance to youths in agriculture and entrepreneurship and revenue generation. The state governments established skill acquisition initiatives, vocational training centres, and empowerment projects to provide citizens with the necessary skills for employment and self-sufficiency. National initiatives such as the Conditional Cash Transfer Programme (CCT) and the Food Support Programme are being implemented to give cash support and food security to needy communities. The planning and implementation of these programmes have hence become a topical issue in academic literature with little or no empirical engagement.

This study examines the impact of SDG One intervention policies and programmes on poverty reduction in Nigeria, with a focus on Osun and Oyo states. It examines the efficiency of poverty reduction initiatives undertaken under SDG One in the

states, and the progress made so far in reducing poverty levels in these states is put under fact check. The potency of SDG One in alleviating extreme poverty in the states by 2030 is thus the thrust of the study.

Objectives of the Study

i. To investigate if there is a disconnect between the planning and implementation of poverty reduction programmes in Osun and Oyo states.
ii. To assess the level of effectiveness of poverty reduction programmes implemented under SDG One in Osun and Oyo states.

Research Hypotheses

i. Ho1: There is no disconnect between planning and the implementation of SDGs poverty reduction programmes in Osun and Oyo states.
ii. Ho2: The poverty reduction programmes under SDG One have no significant impact on poverty reduction in Osun and Oyo states.

Literature Review

Poverty and Poverty Dimensions

The core focus of development cooperation initiatives has perennially centered around the alleviation of poverty. Traditionally, poverty has been perceived solely through a monetary lens, defining an individual as poor if their income fails to meet the minimum threshold required to fulfill basic necessities. This perspective was evident in the Millennium Development Goals (MDGs), particularly in Goal One, Target 1, which aimed to reduce by half the proportion of individuals with a daily income below the USD 1.25 international poverty line established by the World Bank at that time. In recent times, this monetary-centric conceptualization of poverty has encountered robust challenges within the scientific community and from global entities such as the United Nations Development Programme (UNDP) (Burchi, De Muro, and Kollar 2014).

The collaborative study led by Bray R., De Laat M., Godinot X., Ugarte A., and Walker R. (2019) took up a participatory approach involving poor people, practitioners, and academics. Through this inclusive approach, nine common dimensions of poverty were identified. Researchers argue that poverty consists of three dimensions: suffering, disempowerment, and struggle/resistance. Furthermore, three more relationship dimensions further characterize the relationship between people in poverty and people not in poverty: institutional maltreatment, social maltreatment, and unnoticed contributions. Some well-known aspects of deprivation are lack of decent work, insecure income, and material deprivation. Poverty is further complicated by five modifying factors, which include identity, timing/duration, location, environment/policy, and cultural beliefs.

TABLE NO. 1

Poverty Dimensions

LIST OF POVERTY DIMENSIONS DETERMINED BY THE CONSTITUTIONAL APPROACH AND OTHER APPROACHES		
	Most Important Dimensions	**Second-Most Important Dimensions**
Constitutional Approach	Decent work, education, and health	Housing, social security, access to water and food, political participation, access to sanitation, and the environment
Participatory Approach	Decent work, health, and access to food	Access to water, housing, social relations, education, and safety
Survey-Based Approach	Education, health, decent work	Housing, access to water, sanitation, social security, and social relations

Source: (Burchi, De Muro, and Kollar 2018)

Sustainable Development and Sustainability

A crucial prerequisite for achieving sustainable development in any nation lies in maintaining the stability of its natural capital stock. This entails ensuring that present decisions do not compromise the ability to sustain or enhance this capital for future generations. Intergenerational equity emerges as a central concern in the discourse of sustainable development, emphasizing the shared ownership of a nation's resource base across successive generations (Olaniyan, Olatubi, and Ogunbado 2013).

The UN-led sustainable development discourse has evolved over four decades through global summits and comprehensive concept development (Lock and Seele 2017). The 1972 Stockholm United Nations Conference on the Human Environment (UNCHE) was pivotal, establishing sustainable development as balancing human progress with planetary environmental limits (Kates 2015; UNCHE 1972). This conference produced 26 principles on Earth's capacity and socio-economic development, along with an action plan containing 69 recommendations (UNCHE 1972).

Over the two decades spanning from the Stockholm Conference on the Environment to the Rio Conference in 1992, mounting apprehensions have arisen over human activities increasingly imperiling the health of Earth's natural systems, rendering them unsustainable due to irreversible environmental alterations. Presently, a scientific consensus underscores the impermissibility of persisting in these environmentally detrimental activities, recognizing their adverse impacts on ecological conditions necessary for sustained existence (Karpagam 2014).

The term "sustainable development" gained prominence following its introduction by the World Commission on Environment and Development in 1987, marking a pivotal moment in global environmental discourse. Since then, sustainability has emerged as a primary yardstick against which economic development policies are evaluated

by governments, development agencies, and NGOs. Despite the challenges posed by ambiguities in its definition and interpretation, there exists a consensus that sustainable development necessitates proactive government intervention in the efficient and equitable management of natural and environmental resources (Pearson 2013).

Millennium Development Goals (MDGs) and Sustainable Development Goals (SDGs)

The Millennium Development Goals (MDGs) were created in 2000. They aimed at addressing various issues in developing countries. The MDGs encompassed eight goals that focused on poverty, education, gender, health, environment, and many other things (UN 2020). This is useful for a weaker essay. This is what inspired the Rio+20 Conference on Sustainable Development in 2012. Member States agreed that new development goals are needed to build on the MDGs and expand upon them while correcting their shortcomings. This was the goal for the creation of the SDGs. The 2030 Agenda for Sustainable Development was adopted in 2015 by all 193 members of the UN. This gave birth to the Sustainable Development Goals (SDGs) (UNDP 2015). The SDGs are universal, transformative, and inclusive, and address poverty, inequality, climate change, biodiversity loss, and wider issues. Unlike the MDGs, which largely applied to the developing world, the SDGs apply to all countries and recognize that we are all responsible for our planet's well-being. There are 17 SGDs and 169 targets. These include the eradication of poverty, health, education, gender, clean energy, sustainable cities, and responsible consumption and production. The goals are interconnected and mutually reinforcing, emphasizing the need for integrated approaches to development that address the root causes of poverty and inequality while promoting environmental sustainability. And since their adoption, the SDGs have gained widespread recognition and support from governments, civil society, businesses, and international organizations. They provide a common framework for action and cooperation, guiding policy-making, resource allocation, and development efforts at the national, regional, and global levels (UNDP 2015).

Overview of Poverty in Nigeria

Poverty in Nigeria has deep historical roots, beginning with the colonial era when British policies prioritized resource extraction over local development, stifling indigenous industries and laying the groundwork for long-term economic underdevelopment (Falola 2008). After independence in 1960, rapid urbanization and industrialization offered some economic opportunities but also created slum settlements, strained infrastructure, and widened socio-economic disparities (Adepoju 2015). The discovery of oil brought temporary prosperity but entrenched Nigeria's dependence on oil revenues, making the economy vulnerable to global price shocks and discouraging diversification (Omeje 2010). Compounding these challenges, corruption has flourished due to weak governance and institutional inefficiencies, undermining development and diverting public funds from essential services like health, education, and infrastructure (Ojo 2017).

Today, poverty remains widespread in Nigeria, with over 82 million people living below the poverty line (World Bank 2021; NBS 2020). The high rates of unemployment, income inequality, corruption, and poor access to infrastructure account for the causes of the crisis (Aigbokhan 2000; Onakoya 2019; Agbiboa 2013; Bakare 2016; Adeolu 2018; Oluwatobi 2016). The health, education, and food security of people are affected by poverty. Also, various vulnerable groups like women, children, and persons with disabilities also suffer (Ogunlesi 2018; Odhiambo 2017; Ojelabi 2019; Adelekan 2016; Osaghae 2014). Indigenous people in Nigeria generally have lower socio-economic status compared to national averages (Okodua 2015; Amoo 2017; Oyewole 2018). Multidimensional poverty remains a prominent menace as a million Nigerians lack access to clean water, education, health facilities, and food (World Bank 2021; FAO 2021).

Policies, Strategies, and Initiatives by the Nigerian Government to Address Poverty

The Federal Government of Nigeria has employed various policies, strategies, and initiatives to alleviate poverty and promote sustainable development. Some of such are: the National Development Plans, Vision 20:2020, the Economic Recovery and Growth Plan (ERGP), the National Social Investment Programme (NSIP), the National Poverty Eradication Programme (NAPEP) and the National Health Insurance Scheme (NHIS) The First National Development Plan (1962-1968) which aimed to rely more on manufacturing houses to produce essential goods. It envisaged the provision of basic social and economic infrastructures to boost capacity utilization and national productivity (Oyinlola 2016; Ojo 2017). The Second National Development Plan, which was between 1970 and 1974, sought to address the post-civil war reconstruction. Furthermore, it emphasizes rebuilding infrastructure and human capital development. Despite this, there is political instability, which, as a result, did not allow the plan to be successful. Inadequate funding hampered the Second National Development Plan (Falola 2008). The Third National Development Plan, between 1975 and 1980, emphasized the continued growth of industries and infrastructural development. There was a keen focus on improving the standard of living of the people. As part of it, economic diversification and human capital investment were stressed. But policy inconsistencies and external economic shocks reduced its effectiveness (Ajakaiye and Radwan 2010; Aigbokhan 2015; World Bank 2013; Nnadi and Akunyili 2014). The admonition of self-reliance, agricultural development, and rural transformation were the main objectives of the national development plan four (1981–1985). However, governance was weak and funding was low, as well as bureaucratic impediments (Bashir 2015; Adubi 2013; Olayiwola and Adebusuyi 2012; Oyelaran-Oyeyinka and Oyeyinka 2011; Ayinde and Ojo 2017).

The Vision 20:2020 was initiated by the government in 2009 to make Nigeria one of the top 20 global economies by the year 2020. Under this, it was expected to bring about inclusive growth and development. Furthermore, it included various sectors like infrastructure, human capital, and poverty reduction, among

others. Nonetheless, the realization of its aims was hindered by implementation challenges such as a lack of funding, misalignment of polices with economic realities, and external shocks (NPC 2004; Ogwumike and Dada 2013; Osinubi and Amaghionyeodiwe 2014; Ugbaja and Nwezeaku 2019; Salawu and Adeyemi 2015; Olayiwola and Okonkwo 2017; Omodero and Oluwatayo 2018; Ogunsola and Salau 2020; Oluwadare and Olanrewaju 2021; Okorie 2016). The ERGP was designed to create an economy where human and other resources could be used to eradicate poverty and achieve a better life. The focus has been to diversify the economy away from dependence on oil, strengthening the non-oil sectors, besides improvement in infrastructure and social investments. The ERGP was designed with (SDG1) Eradication of Poverty; (SDG5) Gender Equality; (SDG9) Industry, Innovation, and Infrastructure (FGN 2017; Yusuf and Lawal 2019; Adewumi and Adewumi 2018; Oyinlola, Ogundipe, and Adejobi 2020; UNDP 2015; World Bank 2018). The NSIP is the Conditional Cash Transfer (CCT), the National Home-Grown School Feeding Programme (NHGSFP), the Government Enterprise and Empowerment Programme (GEEP), and N-Power, a programme which started in 2016. These programmes that supported the poor and other vulnerable groups, education and health service improvement, and reduction of youth unemployment (Oyinlola, Ogundipe, and Adejobi 2020; Abubakar and Bassey 2019). The National Poverty Eradication Programme (NAPEP) was established in 2001 with the aim of eradicating poverty through training, microcredit, and access to services. Although the programme was much better than before, it faced serious implementation challenges like low funding levels, poor coordination, and corruption (Anyanwu 2013; Ajakaiye, et al. 2015). The National Health Insurance Scheme, NHIS, was established to enhance the accessibility of affordable healthcare and decrease the out-of-pocket health expenditure. A diverse range of studies have suggested that the National Health Insurance Scheme (NHIS) has increased healthcare utilization. Despite this, low enrollment is causing inequitable distribution of services and poor public awareness (Aregbeshola and Khan 2017**;** Onwujekwe, et al 2017).

Oyo State has implemented different programmes following SDG 1 to reduce poverty in the State. According to Adegbola et al (2018), the Oyo State Poverty Alleviation Programme (OYPAP) provides poor groups with money and skill acquisition programmes. Besides, Odeyemi & Adeniran (2019) state that the Oyo State Youth Empowerment Scheme (OYYES) helps youth with entrepreneurship and employment. The Oyo State Microfinance Development Agency (OYSMIDA) gives out microfinance loans and business support. Besides, OYSADEP gives out agricultural support (Akindele, et al. 2017**;** Olawale and Oyekanmi 2020). Other programmes include OYSHIS for health care (Adeyemi, et al. 2019), OYSWP for social welfare (Adeolu and Oladeji 2018), OYESP for education (Oladele and Akanbi 2020) and OYSWEP for women's empowerment (Adeleke and Olawale 2018). Efforts in this regard will help reduce poverty and promote sustainable development in the state. In a similar vein, Osun State has initiated many poverty alleviation programs to achieve the SDGs. This is the Osun State Social Investment Programme (OSSIP), which denotes the Youth Empowerment

Scheme (OYES), and the Elementary School Feeding and Health Programme, O-MEALS, which enhances youth employment and child nutrition (Ajibola and Afolabi 2020; Oyewumi 2018). The Osun State Microcredit Agency (OMA) provides financial assistance to minor entrepreneurs (Ademola and Ayeni 2019) while the Rural Access and Mobility Project (RAMP) enhances rural infrastructure (Oyedokun 2017). The Osun Health Insurance Scheme (OHIS) is to improve access to healthcare and promote the third SDG (Bello, et al. 2020). All these performers will help to achieve the goals of ending poverty (SDG 1), zero hunger (SDG 2), good health and well-being (SDG 3), and decent work and economic growth (SDG 8).

Theoretical Perspective

The study's theoretical framework draws from structural-functionalism and institutional theory to seek answers to questions on the effectiveness of Sustainable Development Goal (SDG) 1, poverty eradication in Osun and Oyo States, Nigeria. Structural-functionalism helps us understand how government agencies, NGOs, community organizations and other social institutions work together to provide services and implement poverty alleviation programmes. As put by Parsons (1951) and Merton (1949), social systems are made up of parts which must work together in units in order to have social stability. It also helps identify structural hurdles be it in terms of bureaucratic inefficiencies (state-specific) or governance challenges that hamper poverty interventions in both states. Despite its merits, structural-functionalism has weaknesses that include overlooking of social conflict, power imbalances, and human agency (Coser 1956; Easton 1957).

Institutional theory complements this analysis by focusing on how both formal structures (laws, agencies) and informal norms shape political behavior, policy implementation, and socio-economic outcomes (March and Olsen 1984; North 1990). The theory aids in understanding how institutional arrangements in Osun and Oyo affect the coordination, resource allocation and monitoring of SDG 1 interventions. While it underscores the importance of administrative capacity and good governance, institutional theory is sometimes critiqued for its deterministic tendencies and limited focus on informal dynamics and sudden political changes (Skocpol 1985; Thelen 1999). In application, the theory provides valuable insights into how institutional strengths and weaknesses, as well as social norms, influence the outcomes of poverty reduction efforts in these states. Together, both theories offer a multidimensional perspective that captures the complexity of achieving poverty eradication through SDG 1 in Nigeria.

Methodology

Research Design

The study adopts a descriptive household survey. Both qualitative and quantitative methods are used. Quantitative data were collected through a household survey questionnaire.

Population of the Study

The population for this study comprised the households in selected local government areas of Osun and Oyo states, Nigeria.

TABLE NO. 2

Twelve Selected Local Government Areas of Osun and Oyo states, their Population and the Number of Households (NBS 5.06 average household size (2019))

S/N	Senatorial Districts	L.G. A	Population	No. of Households
1	**Oyo State North**	SAKI WEST	390,500	77,174
		OLORUNSOGO	116,200	22,964
2	**Oyo State Central**	EGBEDA	405,400	80,119
		OGO-OLUWA	93,200	18,419
3	**Oyo State South**	IBADAN NORTH-EAST	473,700	93,617
		IBARAPA NORTH	143,300	28,320
4	**Osun State West**	IWO	248,400	49,091
		EGBEDORE	96,000	18,972
5	**Osun State East**	IFE-EAST	244,900	48,399
		ATAKUMOSA WEST	88,700	17,530
6	**Osun State Central**	OSOGBO	201,900	39,901
		IFEDAYO	48,700	9,625
	TOTAL		**2,550,900**	**504,131**

Source: Researcher's Field Study (2024)

From the above Table 3.3, the population for the study is **504,131** households scattered across the twelve selected local government areas with **2,550,900** people.

Sample Selection

To arrive at our sample size, the study adopted the Yamane formula. Although there are different types of formulae for determining sample size, the choice of the Yamane formula by this study is to determine the sample size for a finite population.

The formula is as follows:

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

Where:

n = Sample size

N = Total population size

e = Desired level of precision or acceptable sampling error (expressed as a proportion, usually in decimal form)

Sample size calculation for the household population of **504,131**

$$\frac{504,131}{(1+504,131)(0.05)(0.05)}$$

$$\frac{504,131}{(1+504,131)(0.05)(0.0025)}$$

$$\frac{504,131}{(504,132)(0.0025)}$$

$$\frac{504,131}{1260.33}$$

$$= \mathbf{399.99 \approx 400}$$

Using Yamane's formula for a finite population, the sample size of 400 was derived from a household population of 504,131 with a sampling error of 5%. This calculation assumes a 95% confidence level, which is standard for social science research where prior variability is unknown.

Therefore, 400 copies of the household survey questionnaire were administered across the twelve selected local government areas. Copies of the questionnaire allotted to each local government area were calculated using the **Probability Proportionate to Household (PPH) formula**, since the study has adopted the descriptive household survey design.

The PPH formula is as follows:

$$\mathbf{PPH} = \frac{\mathbf{Hp}}{\mathbf{THn}} \times \mathbf{400}$$

Where **Hp** is the individual cluster household number, and **THn** is the total household number for all twelve clusters. Using this formula, the number of copies of the questionnaire for each cluster is generated and presented in Table 3 below:

TABLE NO. 3

Table Showing the Sample Distribution in Selected L.G.As

S/N	L.G. A	No. of Households	No. of Allotted Questionnaire to L.G.A
1	SAKI WEST	77,174	61
2	OLORUNSOGO	22,964	18
3	EGBEDA	80,119	64
4	OGO-OLUWA	18,419	15
5	IBADAN NORTH-EAST	93,617	74
6	IBARAPA NORTH	28,320	22
7	IWO	49,091	39
8	EGBEDORE	18,972	15
9	IFE-EAST	48,399	38
10	ATAKUMOSA WEST	17,530	14
11	OSOGBO	39,901	32
12	IFEDAYO	9,625	8
	TOTAL	**504,131**	**400**

Source: Researcher's Field Study (2025)

Data Presentation and Analysis

TABLE NO. 4

Poverty Reduction Policies and Programmes Implemented Under SDG One in Oyo State and Osun State

	Youth Employment and Social Support Operation (YESSO)	Social Safety Fund	Conditional Cash Transfer	School Feeding Programmes	Government Enterprise and Empowerment Programmes (GEEP) (Trader Money, Market Mon)	State Health Insurance Scheme	Total
Osun State	25 (17.48)	22 (15.38)	25 (17.48)	24 (16.78)	23 (16.08)	24 (16.78)	143 (100)
Oyo State	44 (17.32)	42 (16.54)	42 (16.54)	42 (16.54)	42 (16.54)	42 (16.54)	254 (100)
Total	69 (17.38)	64 (16.12)	67 (16.88)	66 (16.62)	65 (16.37)	66 (16.62)	397 (100)

Source: Field Survey (2025)

Table 4 shows the awareness and participation of households in Osun and Oyo States in six poverty reduction programmes under SDG Goal One, based on a sample of 397 households. The programmes, YESSO, Social Safety Fund, Conditional Cash Transfer, School Feeding Programme, GEEP, and the State Health Insurance Scheme show relatively balanced enrolment rates across the sample, ranging narrowly from 16.12% to 17.38%, indicating no single programme dominates intervention efforts. In Osun State, YESSO and Conditional Cash Transfer recorded the highest participation (17.48%), while the Social Safety Fund was lowest at 15.38%. Oyo State exhibited an even more uniform distribution, with five of six programmes each at 16.54%, and YESSO slightly higher at 17.32%. Comparative analysis reveals only minor differences between the states, suggesting that both implement these programmes in broadly similar ways. Osun shows a slight emphasis on youth employment and cash transfers, while Oyo appears to maintain equitable allocation across all programmes. These small variations reflect localized priorities rather than significant policy differences in SDG 1 implementation.

Hypothesis Ho1: There is no disconnect between planning and the implementation of SDGs poverty reduction programmes in Osun and Oyo states

Variable	Obs	Mean	Std. Err.	Std. Dev.
Planning-Implementation policy disparity scheme disparity employment disparity awareness disparity	397	1.707809	0.031105	0.6197625

t = 22.76 p-value (two-tailed) = 0.000 Null Hypothesis (Ho): Mean = 1 (Strongly Agree there is no disconnect) **Alternative Hypothesis (Ha):** Mean ≠ 1

The one-sample t-test compares the mean score of the variable *Pol_Imp*, which captures perceptions of the alignment between planning and implementation of SDG Goal One, poverty reduction programmes in Osun and Oyo states, against a reference value of 1. On a 5-point Likert scale (1 = Strongly Agree to 5 = Strongly Disagree), a mean of 1 would indicate strong agreement that there is no disconnect, i.e., perfect alignment between planning and implementation. The test result shows that the mean score is 1.71, significantly higher than the benchmark value of 1 with a p-value < 0.001. This leads to the rejection of the null hypothesis, implying that planning and implementation are not well-aligned.

This analysis, Table 4, investigates the disconnect between planning and implementation of poverty reduction programme in Osun and Oyo states by comparing the mean values of four key indicators: policy disparity (respondents' average rating on policy

TABLE NO. 5

Disconnect between planning and implementation of poverty reduction programme in Osun and Oyo states (Comparative Analysis)

State	Ho = mean (Osun State) – mean (Oyo State)			
	Policy (mean)	Awareness (mean)	Scheme (mean)	employment (mean)
Osun State	2.561772	3.825175	3.018648	3.286713
Oyo State	2.423885	3.799213	3.082677	3.830709
Combined	2.473552	3.808564	3.059614	3.634761
Diff	0.1378871	0.0259622	-0.0640291	-0.5439954
t-statistic	2.7443***	0.2719	-1.1429	-5.536***

Source: Field Survey (2025) *** *p<.01*, ** *p<.05*, * *p<.1*

related aspects of poverty programme), awareness disparity (Level of awareness about these programme), scheme disparity (perception or knowledge about specific schemes or initiatives), and employment disparity (views on how these programme impact employment or job opportunities). These indicators represent how far actual implementation deviates from planning intentions in different aspects of programme delivery in Osun and Oyo states. The findings show that there are variant disconnects between planning and implementation across the key indicators used. The statistically significant positive difference indicates that Osun State exhibits a higher policy level disconnect than Oyo State. This suggests that in Osun State, there is a notable gap between policy formulation and operational execution.

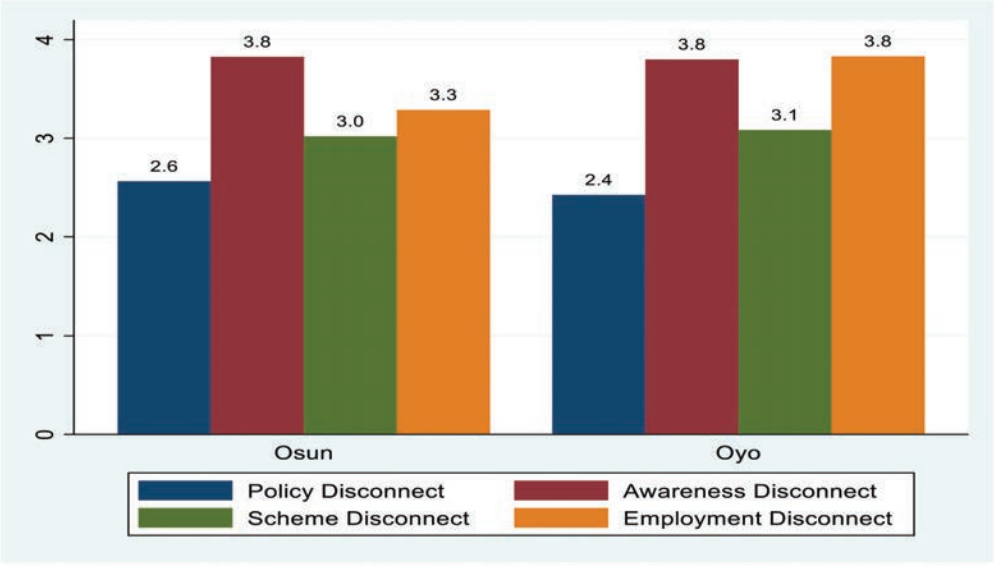

Figure 1 Disconnect between planning and implementation of poverty reduction programme in Osun and Oyo states
Source: Field survey (2024)

The bar chart, Figure 1, presents the mean levels of disconnect across four key components of the poverty reduction programme, Policy, Awareness, Scheme, and Employment in Osun and Oyo states. These disconnects represent the gaps between planning and implementation, providing insights into the effectiveness of poverty

alleviation efforts in both states. Although both states report relatively low levels of policy disconnect, Osun State's slightly higher value suggests a marginally greater gap between policy formulation and its practical application. This reflects ambitious planning documents that are not adequately backed by execution capacity. However, the difference is not substantial.

Hypothesis Ho2: The poverty reduction programmes under SDG One have no significant impact on poverty reduction in Osun and Oyo states

Variable	Obs	Mean	Std. Err.	Std. Dev.
Pov_Int	397	2.516	0.0181	0.3609

t-statistic = 83.70, p-value (two-tailed) = 0.000

The mean score of 2.52 on a scale where 1 = Strongly Agree and 5 = Strongly Disagree suggests that, on average, respondents tend to disagree with the statement that SDG One poverty reduction programmes have had no significant impact. In simpler terms, this implies that respondents perceive the interventions as having some meaningful effect on poverty reduction, though not strongly. The t-value of 83.70 and a p-value of 0.000 indicate that the result is statistically significant at the 1% level. Therefore, we reject the null hypothesis and conclude that the poverty reduction programmes under SDG One have a significant impact on reducing poverty in Osun and Oyo states. The level of impact is low.

TABLE NO. 6

Level of Effectiveness of Poverty Reduction Programmes Under SDG One in Osun and Oyo states

Poverty	Coef.	St.Err.	t-value	p-value
Income_Support	0.062	0.169	0.37	0.713
Service_Access	-0.273**	0.138	-1.98	0.048
Health_Support	0.179*	0.104	1.72	0.085
Employment	-0.039	0.068	-0.57	0.569
Constant	1.119**	0.973	1.15	0.025
Mean dependent var	0.637	SD dep var		0.481
Pseudo r-squared	0.013	Number of obs		397
Chi-square	6.952	Prob > chi2		0.138
Akaike crit. (AIC)	523.092	Bayesian crit. (BIC)		543.011
*** $p<.01$, ** $p<.05$, * $p<.1$				

Source: Field Survey (2025)

Probit regression analysis was used to assess the effectiveness of the poverty reduction programme under SDG One in Osun and Oyo states, using a sample of

397 households as depicted in Table 4.9. The model evaluated four dimensions of intervention: Income Support, Service Access, Health Support, and Employment Initiatives. Income Support exhibited a positive coefficient (0.062), but the relationship was statistically insignificant (p = 0.713). This indicates that direct financial assistance programmes have not had a meaningful impact on poverty reduction among the respondents.

Service Access emerged as the only significant predictor with a negative coefficient (-0.273), significant at the 5% level (p = 0.048). This suggests that inadequate access to essential services such as healthcare, education, and public utilities significantly reduces the likelihood of escaping poverty. Health Support showed a positive coefficient (0.179) and was marginally significant at the 10% level (p = 0.085). This result indicates that access to healthcare moderately improves the probability of poverty reduction, albeit with weaker statistical support. Employment Initiatives, however, had a negative but statistically insignificant effect (-0.039, p = 0.569), implying that employment-related interventions, as implemented, did not significantly influence poverty reduction. The overall model fit was good, with a Chi-square statistic of 69.52 (p = 0.018), indicating that the set of predictors does jointly explain poverty reduction outcomes at a conventional significant levels.

Summary of the Findings

The study reveals a significant disconnect between planning and implementation in Nigeria's poverty alleviation efforts, revealing disparities across policy, schemes, employment, and public awareness. While policies are often well-designed, their execution is undermined by poor coordination, weak data systems, limited institutional capacity, and political interference. In Oyo State, employment initiatives, particularly youth empowerment programmes, have failed to yield tangible results due to exclusion of local actors and logistical inefficiencies. Although some interventions show modest positive effects, the overall impact remains limited. Of the four intervention areas; Income Support, Service Access, Health Support, and Employment, only Service Access showed a statistically significant impact, and it was negatively associated with poverty reduction, underscoring the role of inadequate infrastructure and service delivery. These findings reflect broader critiques of Nigeria's poverty reduction strategies, which are hindered by structural flaws such as fragmented implementation, policy inconsistency, and institutional weakness.

Conclusion

Drawing upon both quantitative and qualitative data, the study affirmed that the limitations confronting Nigeria's efforts in reducing poverty under SDG 1 are not rooted in policy absence but in weak governance structures, suboptimal implementation practices, and systemic gaps in stakeholder coordination and monitoring. Despite the widespread deployment of SDG-aligned poverty reduction

programmes such as Conditional Cash Transfer (CCT), Government Enterprise and Empowerment Programme (GEEP), Youth Employment and Social Support Operations (YESSO), and the School Feeding Scheme, their impacts have largely been palliative rather than transformative. These interventions offer short-term assistance but fall short in addressing the deep-rooted and multidimensional nature of poverty across urban and rural areas in both states. While the design of these programmes is well-intentioned, poor targeting and a lack of sustainability planning severely hinder their effectiveness.

Recommendations

To bridge the disconnect between planning and implementation of poverty reduction programmes in Osun and Oyo States, the study recommends the creation of robust coordination mechanisms, including multi-stakeholder task forces involving government, civil society, and community leaders to co-design practical, locally adaptable strategies. Emphasis should be placed on accurate, community-specific data from sources like State Operation Coordinating Units (SOCU) to reduce errors and delays in programme delivery. Employment initiatives should be reformed through demand-driven vocational training, post-training job placement, and partnerships with the private sector, while monitoring systems must be digitized for real-time feedback and accountability. Addressing awareness gaps is equally crucial, requiring structured communication strategies that engage grassroots actors in local languages, deploy mobile outreach units, and offer multilingual support services to foster inclusive participation. To improve the effectiveness of SDG One programmes, governments must shift focus from short-term interventions to sustainable service delivery by investing in infrastructure, improving inter-agency coordination, and ensuring services reach marginalized communities.

References

Abubakar, A., and M. Bassey. 2019. "Evaluation of the National Social Investment Programme (NSIP) on Education Outcomes in Nigeria." *Journal of Educational Administration and Policy Studies* 11(1): 1-12.

Adebusuyi, B.S. 1985. *Economic Planning in Nigeria: The First and Second National Development Plans.* Macmillan Nigeria Publishers.

Adegbola, O.O., et al. 2018. "An Assessment of Poverty Alleviation Programmes in Oyo State, Nigeria." *International Journal of Humanities, Art and Social Studies* 3(6): 13-21.

Adelekan, I.O. 2016. "Gender, Poverty and Social Exclusion in Nigeria: Towards an Inclusive Transformation Agenda." *Journal of Poverty, Investment and Development* 26: 88-98.

Ademola, A.S., and M.T. Ayeni. 2019. "Microfinance intervention and poverty alleviation: Evidence from Osun State, Nigeria." *Journal of Research in Business, Economics and Management* 15(4): 27-33.

Adeolu, O. 2018. "Infrastructure Development and Poverty Alleviation in Nigeria: An Empirical Analysis." *International Journal of Economics, Commerce and Management* 6(2): 41-58.

Adeolu, R.A., and O.S. Oladeji. 2018. "Social Welfare Programmes and Poverty Reduction in Oyo State, Nigeria." *International Journal of Sociology and Anthropology* 10(1): 1-10.

Adepoju A. 2005. "Migration in West Africa. A paper prepared for the Policy Analysis and Research Programme of the Global Commission on International Migration." https://www.iom.int/sites/g/files/tmzbdl2616/files/2018-07/RS8.pdf

Adewumi, M.O., and A.O. Adewumi. 2018. "Economic Diversification and Sustainable Growth in Nigeria: The Role of the Manufacturing Sector." *Journal of Economics and Sustainable Development* 9(12): 150-160.

Adeyemi, O. I., et al. 2019. "Health Insurance Scheme and Access to Healthcare Services in Oyo State, Nigeria." *International Journal of Health Sciences and Research* 9(6): 209-217.

Adubi, A.A. 2013. Agricultural Transformation Agenda and Food Security in Nigeria. *International Journal of Agriculture and Rural Development* 16(1): 1279-1285.

Agbiboa, D.E. 2013. "Corruption and Development in Africa: Challenges for Political and Economic Change." *African Conflict and Peacebuilding Review* 3(2): 96-123.

Aigbokhan, B.E. 2000. "Poverty, growth, and inequality in Nigeria: A case study." *Economic and Financial Review* 38(4): 1-13.

___. 2015. *The Challenges of Human Capital Development in Nigeria*. In F. O. Ojukwu & P. C. Ukpabi (Eds.), *Human Capital Formation and Economic Growth in Nigeria: The Role of Education, Health, Agriculture and Industrial Policies*. Springer.

Ajakaiye, O., and S. Radwan. 2010. *Nigeria: Macroeconomic Performance and Policy Framework for the Short and Medium Term.* African Economic Research Consortium.

Ajakaiye, O., A. Jerome, D. Nabena, and F. Alaba. 2015. Understanding the relationship between growth and employment in Nigeria (WIDER Working Paper 2015/124). United Nations University World Institute for Development Economics Research (UNU-WIDER). https://doi.org/10.35188/UNU-WIDER/2015/013-3

Ajibola, O.S., and A.O. Afolabi. 2020. *Youth Empowerment Programme and Unemployment Reduction in Nigeria: A Study of the Osun State Youth Empowerment Scheme.* In Handbook of Research on Unemployment and Labor Market Sustainability in the Era of Globalization (pp. 241-259). IGI Global.

Amoo, B. 2017. "Poverty Alleviation Programme and the Sustainable Development Goals in Nigeria." *Journal of Economics and Sustainable Development* 8(3): 88-97.

Anyanwu, J.C. 2013. "Poverty Reduction Strategies in Nigeria: Lessons from Past Development Initiatives." *African Development Review* 9(2): 215-230.

Anyanwu, J.C., A. Oyefusi, H. Oaikhenan, and F.A. Dimowo. 1997. *The structure of the Nigerian economy (1960 –1997).* Onitsha: Joanee Publisher.

Ayida, A.A. 1987. *Reflection on Nigeria's development.* Lagos: Malthouse Press.

Ayinde, O.E., and T.O. Ojo. 2017. "Rural Transformation Agenda and Food Security in Nigeria." *Journal of Agricultural Extension* 21(1): 129-139.

Ayo, E.J. 1988. *Development planning in Nigeria.* Ibadan: University Press.

Bakare, S.A. 2016. "Corruption and Poverty in Nigeria: A Cause-Effect Relationship." *Journal of Poverty, Investment and Development* 26: 109-120.

Bashir, A. 2015. "Self-Reliance and the Nigerian Economy: A Comparative Analysis of the Second and Fourth National Development Plans." International *Journal of Development and Sustainability* 4(3): 124-142.

Bello, B., A. Adeoti, A. Adeniran, and O. Adewumi. 2020. "Impact of National Health Insurance Scheme on Access to Healthcare in Osun State, Nigeria." *Open Journal of Medical Microbiology* 10(2): 49-61.

Bray, R., M. De Laat, X. Godinot, A. Ugarte, and R. Walker. 2019. "Exploring the multidimensional dimensions of poverty: A participatory study." *Journal of Poverty Studies* 21(3): 45-67.

Burchi, F., P. De Muro, and E. Kollar. 2014. "Rethinking poverty: Beyond monetary measures." *Global Social Policy* 14(1): 11-30.

___. 2018. "Unveiling the essence of poverty: A constitutional approach." *Global Development Journal* 12(2): 89-104.

Coser, L.A. 1956. "The functional prerequisites of social systems." *Sociological Inquiry* 26(2): 150-155.

Dodo, R.O. 2010**.** Yar'Adus's Seven-point agenda, the MDGs and sustainable development in Nigeria. *Global Journal of Human Social Sciences* 10(4).

Easton, David. 1957. *A Framework for Political Analysis.* Englewood Cliffs, New Jersey: Prentice Hall.

Falola, T. 2008. "Economic Development and Reform in Nigeria: From the Colonial Era to the Present." *African Economic History* 36: 99-120.

Federal Government of Nigeria (FGN) 2014. "The transformation agenda 2011-2015." Retrieved from www. budgetoffice.gov.ng

Federal Republic of Nigeria (FRN). 2012. *Subsidy reinvestment and empowerment programme (SURE-P).* 2012 Annual Report. Retrieved on 07/01/2021 from www. sure-p.gov.ng/

Food and Agriculture Organization of the United Nations (FAO). 2021. *The State of Food Security and Nutrition in the World 2021.*

Ibeanu, O. 2004. "Alternative poverty eradication strategy. Introductory issues." In *The Centre for Democracy and Development (Ed.).* Alternative Poverty Reduction Strategy for Nigeria.Lagos: CDD.

Igbuzor, O. 2004. "Poverty eradication and public policy in Nigeria." In *The Centre for Democracy and Development (Ed.).* Alternative Poverty Reduction Strategy for Nigeria. Lagos: CDD

Ijaiya, G.T. and M.A. Nuhu. 2011. "Low education attainment and the incidence of poverty in Ilorin metropolis, Nigeria." *International Journal of Social Sciences and Humanities* 2 (1): 81- 90.

Karpagam, R. 2014. "Sustainable development: Issues and challenges." *Virtue Journals* 19(3): 186-198.

Kates, R.W. 2015. "What kind of science is sustainability science?" *Proceedings of the National Academy of Sciences* 112(31): 9532-9534.

Kharas, H., and M. Dooley. 2022. *The evolution of global poverty, 1990–2030* (Brookings Global Working Paper No. 166). Brookings Institution. https://www.brookings.edu/SustainableDevelopment

Lock, A., and P. Seele. 2017. "The United Nations sustainable development goals: Achieving the vision of global health with justice." *Global Health Action* 10(1).

March, J.G., and J.P. Olsen. 1984. *Organizing political life: What administrative reorganization tells us about government*. University of Michigan Press.

Merton, Robert K. 1957. *Social Theory and Social Structure.* New York: The Free Press.

National Bureau of Statistics (NBS). 2020. "Poverty and Inequality in Nigeria 2019." https://www.nigerianstat.gov.ng/elibrary/read/1092

___. 2022. "Multidimensional Poverty Index 2022: Report for Nigeria." https://www.nigerianstat.gov.ng/pdfuploads/NIGERIA%20MULTIDIMENSIONAL%20POVERTY%20INDEX%20SURVEY%20RESULTS%202022.pdf

National Planning Commission (NPC). 2004. *National economic empowerment and development strategy (NEEDS).* Abuja, Nigeria: NPC.

___. 2009. *National Economic Empowerment and Development Strategy: A Nationally Consensus Building Economic Empowerment Strategy for Nigeria*. Abuja, Nigeria: NPC.

National Social Safety Net Office (NASSCO). 2020. "National social investment programme." Retrieved from www.nassp.gov.ng.

National Social Investment Office (NSIO) 2016. "National social investment programme." https://www.statehouse.gov.ng/policy/economy/national-social-investment-programme/

Nnadi, S.C., and C.N. Akunyili. 2014. "An Evaluation of the Third National Development Plan (1975-1980) and Its Implications for Sustainable Development in Nigeria." *International Journal of Academic Research in Business and Social Sciences* 4(6): 81-95.

Odeyemi, A.O., and O.A. Adeniran. 2019. "Youth Empowerment and Economic Development in Oyo State, Nigeria." *International Journal of Scientific Research and Education* 7(11): 2547-2556.

Odihiambo, W.O. 2017. "The Impact of Poverty on Education in Nigeria." *Journal of Educational and Social Research* 7(2): 67-78.

Ogunlesi, T.A. 2018. "Poverty and Healthcare Access in Nigeria: An Exploratory Study." *Nigerian Journal of Medicine* 27(1): 76-88.

Ogunsola, A.A., and A.S. Salau. 2020. "Human Capital Development and Economic Growth in Nigeria: An Empirical Analysis." *Journal of Economics and Sustainable Development* 11(5): 1-11.

Ogwumike, F.O. 2001. "Appraisal of poverty and poverty reduction strategies in Nigeria." *Central Bank of Nigeria (CBN) Economic and Financial Review* 39(4): 45-71.

Ogwumike, F.O., and E.O. Dada. 2013. "Vision 20:2020 and Sustainable Development in Nigeria." *Journal of Sustainable Development in Africa* 15(7): 82-94.

Ojelabi, R.A. 2019. "Dimensions of Poverty and Social Exclusion in Nigeria: A Review." *Journal of Economics and Sustainable Development* 10(6): 85-94.

Ojo, S.O. 2017. "Corruption and Economic Development in Nigeria: A Contemporary View." *African Development Perspectives Yearbook* 24: 125-140.

Okodua, H. 2015. "Poverty in Rural Nigeria: Perceptions and Realities." *Journal of Economic and Social Studies* 5(2): 109-125.

Okorie, C.N. 2016. "Challenges of Implementation of Nigeria's Vision 20:2020." *International Journal of Humanities and Social Science Invention* 5(7): 66-73.

Oladele, T.O., and A.A. Akanbi. 2020. "Educational Support Programmes and Poverty Alleviation in Oyo State, Nigeria." *Journal of Education and Practice* 11(4): 1-10.

Olaniyan, O.S., W.O. Olatubi, and A.F. Ogunbado. 2013. "Intergenerational equity in the governance of natural resources in Africa: The case for oil and gas." *African Journal of Environmental Science and Technology* 7(8): 711-720.

Olawale, A.O., and O.E. Oyekanmi. 2020. "Microfinance Banks and Economic Empowerment of Small-Scale Enterprises in Oyo State, Nigeria." *African Research Review* 14(3): 445-458.

Olayide, S.O. 1976. *Economic survey of Nigeria (1960 –1975)*. Ibadan: Aromolaran Publishing Co.

Olayiwola, K.O., and B.S. Adebusuyi. 2012. "Food Security in Nigeria: The Role of Agriculture." *European Journal of Sustainable Development* 1(2): 251-264.

Olayiwola, K.O., and R. Okonkwo. 2017. "Infrastructure Development and Economic Growth in Nigeria: A Time Series Analysis. *Journal of Economics and Sustainable Development* 8(14): 157-166.

Ole, R. 2009. Yar'Adus's Seven-point agenda: Any hope for the Nigerian people. Retrieved from www.marxium.com.

Oluwadare, O.J., and R.I. Olanrewaju. 2021. "Evaluation of Vision 20:2020 as a Framework for Sustainable Development in Nigeria." *Journal of Humanities and Social Science Research* 3(1): 45-54.

Oluwatobi, S. 2016. "Infrastructure and Poverty Reduction in Nigeria: An Empirical Analysis." *Journal of Economics and Sustainable Development* 7(2): 45-58.

Omeje, K. 2010. "Nigeria's Oil Conflict and Resolution Strategies: Beyond Resource Curse Paradigms." *Journal of Asian and African Studies* 45(4): 407-428.

Omodero, C.O., and J.A. Oluwatayo. 2018. Human Capital Development and Economic Growth in Nigeria: An Empirical Investigation. *International Journal of Economics, Commerce and Management* 6(6): 329-341.

Onakoya, A.B. 2019. "Unemployment and Poverty in Nigeria: An Empirical Study." *Journal of African Studies and Sustainable Development* 5(2): 98-113.

Osaghae, E.E. 2014. "Nigeria's Uneven Development: An Evaluation of Poverty, Inequality and Unemployment Trends in the Fourth Republic." *Africa Development* 39(3): 123-138.

Osinubi, T. S., and L.A. Amaghionyeodiwe. 2014. "Poverty and Income Inequality in Nigeria: Any Causal Relationship?" *African Development Review* 26(S1): 112-141.

Oyedokun, T.T. 2017. "Impact of Rural Access and Mobility Project (RAMP) on Rural Infrastructure Development in Osun State, Nigeria." *International Journal of Management and Humanities* 2(1): 10-21.

Oyelaran-Oyeyinka, B., and B.O. Oyeyinka. 2011. "Rural Development Policies and Sustainable Development in Nigeria: An Appraisal." *Africa Development* 36(1): 131-152.

Oyewole, O. 2018. *Social exclusion and indigenous populations in Nigeria*. Abuja: National Institute for Policy Studies.

Oyewumi, K. 2018. "School Feeding Programme and the Academic Performance of Primary School Pupils in Osun State, Nigeria." *Journal of Research in Education and Society* 9(3): 98-107.

Oyinlola, A. 2016. "Industrialization in Nigeria: Challenges and Opportunities." *Journal of Economics and Sustainable Development* 7(1): 54-65.

Oyinlola, M.A., A.A. Ogundipe, and A.O. Adejobi. 2020. "Evaluating the National Social Investment Programme (NSIP) in Nigeria: Lessons and policy implications." *Nigerian Journal of Economic and Social Studies* 62(1): 121-139.

Parsons, T. 1951. *The social system.* Routledge.

Pearson, K. 2013. "The politics of environmental sustainability: Sustainability as a political quantity." *Environmental Politics* 22(1): 41-60.

Salawu, B., and T.O. Adeyemi. 2015. "Infrastructure Development and Economic Growth in Nigeria: The Role of Foreign Aid." *Journal of Business and Economic Development* 3(2): 47-57.

Skocpol, T. 1985. *Bringing the State Back In: Strategies of Analysis in Current Research.* In Evans, Peter B., Rueschemeyer, Dietrich and Skocpol, Theda. (Eds.), Bringing the State Back In. Cambridge University Press.

Thelen, K. 1999. "Historical institutionalism in comparative politics." *Annual Review of Political Science* 2: 369-404.

Ugbaja, S.S., and N.C. Nwezeaku. 2019. "Vision 20:2020 and Poverty Reduction in Nigeria: An Assessment." *Journal of Economics and Sustainable Development* 10(9): 156-166.

United Nations (UN). 2020. *The Sustainable Development Goals Report 2020.* New York, NY: United Nations.

United Nations Conference on the Human Environment (UNCHE). 1972. "Environment and sustainable development." https://www.un.org/en/conferences/environment.

United Nations Development Programme (UNDP). 2015. "Sustainable Development Goals."

World Bank. 2013. *Nigeria: Building a Competitive Economy for Sustained Growth.* World Bank Publications.

___. 2018. *Nigeria Economic Update: Inclusion Matters - The Path to a Prosperous Nigeria.*

___. 2021. *Poverty in Nigeria: Understanding and Overcoming the Challenge.* World Bank Group.

Yusuf, T.M., and A.M. Lawal. 2019. "Economic Recovery and Growth Plan (ERGP): A Panacea for Nigeria's Economic Downturn." *Journal of Economics and Sustainable Development* 10(4).

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Hybrid Security and the Erosion of State Monopoly: Vigilantism, Informal Security and Political Order in the Lake Chad Basin

Emmanuel Oyewole LAMBE*

*Department of International Relations, Ahman Pategi University, Patigi, Nigeria
e-mail: Emmanuel.lambe60@gmail.com
https://orcid.org/0009-0002-9459-602X

Abstract

This study investigates the evolving security architecture of the Lake Chad Basin through the lens of hybrid security governance and the erosion of the state's monopoly on violence. In the aftermath of the unchecked Arab Spring conflicts, the region's historically porous borders, especially along Northern Nigeria and the broader Sahel, became conduits for the diffusion of armed groups, religious extremism, and illicit arms. Longstanding issues of ethnic intolerance, political marginalisation, and chronic state neglect intensified an already fragile context, creating ungovernable spaces where vigilante groups and communal militias have emerged as de facto security providers. In many rural areas around the Lake Chad shores, communities have taken up arms not in rebellion, but in rejection of a state that has largely abdicated its protective function. However, this rise in non-state security actors complicates the legitimacy of formal security frameworks, disrupts national sovereignty, and transforms the nature of political order. The research adopts a mixed-methods approach. Data were gathered through interviews with key stakeholders, questionnaires administered across four Lake Chad-adjacent states, content analysis of media reports, and panel data (2020–2025) on vigilante activity and trust indices. Findings show that vigilante groups have proliferated in direct response to state neglect and ungoverned territories, but their operations, while locally legitimised, often challenge state authority and blur lines of accountability. The study draws on the principle that political vacuums invite informal authority structures, applying this to theorise a model of complementary insecurity. It concludes with recommendations including internal border reform, integrated intelligence frameworks, and community-state security compacts to navigate the emerging plural security order.

Keywords:
Hybrid Security; Governance; Vigilantism; Informal Security Actors; Political Order.

Article info
Received: 7 July 2025; Revised: 4 August 2025; Accepted: 2 September 2025; Available online: 6 October 2025

Citation: Lambe, E.O. 2025. "Hybrid Security and the Erosion of State Monopoly: Vigilantism, Informal Security and Political Order in the Lake Chad Basin." *Bulletin of "Carol I" National Defence University*, 14(3): 101-123. https://doi.org/10.53477/2284-9378-25-38

The Lake Chad region has emerged as a crucible of persistent insecurity, defined by insurgency, state fragility, and the proliferation of non-state security actors. Stretching across the borders of Nigeria, Chad, Cameroon, and Niger, the region has witnessed a marked rise in complementary security structures, including vigilante groups and local militias, operating alongside or in lieu of formal state forces (ICG 2017; Bukarti 2020). These actors have not only become de facto security providers in ungoverned and under-governed spaces but have also reshaped the architecture of local and regional security governance (Debos 2016).

The rise of these vigilante groups is not incidental but rather symptomatic of deeper structural deficits, including the existence of vast ungovernable terrains (Reno 2011), the erosion of state monopoly over violence (Weber 1946), and the security vacuums that have emerged due to delayed or inadequate state responses (Hoffmann and Kirk 2013). These vacuums were further widened by the ripple effects of the Arab Spring, which destabilized the Sahel and precipitated arms proliferation, insurgent mobility, and the weakening of already brittle state institutions (Lacher 2012; Marchal 2013). In many cases, the state's failure to proactively intervene or its outright neglect has necessitated grassroots forms of security mobilisation, often justified as self-defence or communal protection (Roitman 2005; Bøås and Dunn 2007).

Moreover, recurring ransom economies, enabled by state reluctance to confront armed groups decisively, have further delegitimised formal institutions (Hansen and Sæther 2021). Complacency and complicity among military personnel, manifested through repeated allegations of aiding insurgents or turning a blind eye, have only deepened public distrust and accelerated the turn towards alternative security providers (Akinola 2020a; Péclard and Mechoulan 2015). These dynamics align with the theoretical insights from the security governance literature, which explains how, in fragmented sovereignty contexts, security provision becomes a polycentric and negotiated process rather than a centralised state function (Baker and Scheye 2007; Hills 2009).

Beyond the immediate localities of the Lake Chad basin, this trend raises profound questions within international relations, especially regarding the diffusion of insecurity, the erosion of Westphalian sovereignty, and the transnational implications for border governance, counter-terrorism cooperation, and migration control (Clapham 1996; Buzan and Wæver 2003; Bilgin and Morton 2002). Western powers, particularly those invested in the Global War on Terror and regional stability in the Sahel, are increasingly drawn into these dynamics, whether through military assistance, policy partnerships, or humanitarian intervention (Williams 2013; Raineri 2020). As such, the phenomenon of vigilante and community-led security in the Lake Chad region cannot be understood in isolation but must be situated within the global discourse on hybrid security and the changing norms of intervention and sovereignty in postcolonial states (Leonard 2013; Duffield 2007).

This study, therefore, interrogates the emergence, operation, and implications of complementary security actors in the Lake Chad region. It focuses on the causal factors (ungovernable spaces, governance vacuums, and external geopolitical shocks), the necessity drivers (state neglect, delayed intervention, ransom negotiations, and institutional complicity), and the broader international reverberations that place the Lake Chad security crisis on the global agenda. By doing so, it contributes both to empirical understanding and theoretical debates within security studies, peacebuilding, and international relations.

Research Question

What are the structural and geopolitical factors that have driven the rise of vigilante and complementary security groups in the Lake Chad region, and how do these actors reshape both local security dynamics and international responses to regional instability?

Sub-questions

1. How have ungovernable spaces, state neglect, and delayed intervention contributed to the rise of vigilante groups in the region?
2. What role do military complicity and the persistence of ransom economies play in legitimising non-state security providers?
3. How have the Arab Spring and other external geopolitical disruptions influenced the securitisation landscape in Lake Chad?
4. What are the implications of this security pluralism for international security frameworks and state sovereignty?

Conceptual Clarifications

Complementary Security

Complementary security refers to non-state or community-based security initiatives that operate alongside, or in place of, formal state security structures to provide safety, surveillance, and order within local jurisdictions. In conflict-affected or neglected regions like Lake Chad, these formations emerge to fill critical protection gaps left by state absence or inefficiency. Unlike parallel security (which may challenge state legitimacy), complementary security tends to be tolerated or even informally sanctioned by state actors, despite lacking formal legal authority (Baker 2009; Hills 2016).

In contexts such as northeastern Nigeria, this includes formations like the Civilian Joint Task Force (CJTF), local hunters, and neighborhood watch coalitions who, despite lacking constitutional mandates, have become central actors in controlling territory and intelligence gathering. These actors do not replace the state wholesale but fill functional vacuums often with the tacit or active approval of government and

international security institutions. As such, complementary security should be seen as a hybrid governance mechanism, not an aberration but a patterned response to crisis in peripheral zones of weak states (Meagher 2012; Lund 2006).

Ungovernable Spaces

Ungovernable spaces are territories where the state lacks effective authority or capacity to enforce law, deliver services, or maintain security (Risse 2011; Clunan and Trinkunas 2010). These spaces may be geographically remote, economically marginal, or contested by armed groups. In the Lake Chad Basin, ungovernable spaces have been shaped by colonial border fragmentation, climate-induced displacement, and the weakening of administrative infrastructures, leading to power vacuums often filled by insurgents, militias, or vigilante actors.

The Lake Chad region exemplifies this, as significant parts of Borno, Diffa, and Far North Cameroon have cycled in and out of state control. What makes these spaces "ungovernable" is not only territorial loss but institutional vacuity, a lack of service delivery, justice access, and infrastructural presence. This condition creates fertile ground for both insurgency and community-based defense networks (Clunan and Trinkunas 2010).

Local Intelligence

Local intelligence denotes community-based knowledge networks used to monitor, report, and prevent security threats, especially in areas where formal surveillance is weak. It includes informal communication channels, traditional informants, and cultural awareness that enable early warning and tactical coordination. Vigilante groups often depend on this form of intelligence for both defensive and offensive operations, which state forces may come to rely on or co-opt (Ubhenin 2014; Onuoha 2010).

Local intelligence refers to community-based gathering, monitoring, and relay of information about threats, especially where formal surveillance or military intelligence is absent or ineffective. In complementary security arrangements, local intelligence plays a foundational role, often outperforming formal actors due to intimate knowledge of local dynamics, actors, and terrain.

Actors like the CJTF in Nigeria or vigilante networks in northern Cameroon have been instrumental in identifying insurgent collaborators, mapping movement corridors, and detecting sleeper cells. However, such systems often operate without legal frameworks or transparency, and are vulnerable to abuse, misinformation, and ethnic profiling, especially when driven by local rivalries or grievances (Agbiboa 2015; Onuoha 2010).

Vigilante Justice

Vigilante justice is a form of extra-legal enforcement where individuals or groups undertake punitive or preventive action in the absence, or perceived failure of, formal

legal systems. In the Lake Chad region, vigilante groups such as the Civilian Joint Task Force (CJTF) engage in surveillance, arrest, and even execution of suspected insurgents, often without due process. While sometimes effective in containing threats, vigilante justice often results in human rights violations and undermines the rule of law (Agbiboa 2015; Meagher 2012).

In the Lake Chad region, vigilante justice is characterized by swift enforcement, personalized accountability, and local legitimacy, often based on ethno-religious or communal ties. While it may offer immediate protection or retribution, vigilante justice often lacks procedural safeguards and can reproduce cycles of violence, exclusion, and impunity. It is critical to distinguish between defensive vigilantes (who seek to protect communities) and punitive vigilantes (who exact retribution), even though both often coexist within the same groups (Rosenbaum and Sederberg 1974; Abrahams 1998).

Communal Military Response (CMR) Units

CMR units refer to community-organised armed groups formed to defend local populations against external threats, often under the guidance of traditional authorities or local elites. Unlike spontaneous mobs, CMRs may be semi-structured, trained in rudimentary combat, and possess command hierarchies. In the Lake Chad region, these units play a dual role: resisting insurgent incursions and asserting local autonomy over the terms of security and protection (Debos 2016; Péclard and Mechoulan 2015).

Communal Military Response (CMR) units are localized paramilitary or quasi-military organizations, often emerging from community self-defense traditions. They tend to be militarily organized, disciplined, and sometimes uniformed or armed, resembling militias more than civilian vigilante groups. Their authority stems from community mandate rather than constitutional legitimacy.

CMRs are more than mere vigilantes; they represent structured militarization of community security and often coordinate directly with state forces. In Niger's Diffa region and parts of Chad, such formations have been absorbed into broader national security efforts, though often without formalized training or oversight. Their rise reflects not just a security gap, but also the gradual informalization of state sovereignty in peripheral zones (Debos 2016).

Marginalised Groups

Marginalised groups are social categories systematically excluded from political, economic, or security participation. In Lake Chad, ethnic minorities, pastoralist communities, and internally displaced persons often fall into this category. Their exclusion from state protection compels some to either join armed groups for survival or support vigilante formations as alternative power structures. Marginalisation thus becomes both a driver and consequence of informal security proliferation (Ikelegbe 2005; Idris 2018).

Many complementary security formations are drawn from or mobilized by such groups, either to protect themselves from insurgents or to assert claims to citizenship and recognition. However, their marginality also increases their vulnerability to co-optation, exploitation, or criminalization, particularly when the state reasserts control or when donor policies shift (Idris 2018).

Theoretical Review

1. State Failure Theory

State Failure Theory posits that insecurity and the proliferation of alternative governance structures arise when a state loses its monopoly over the legitimate use of force and fails to provide core public goods such as protection, justice, and welfare (Rotberg 2004; Zartman 1995). A failed or failing state is unable to project authority over its territory, leading to security vacuums that are rapidly filled by non-state actors, including militias, vigilantes, and insurgents.

In the Lake Chad region, persistent failure by the states of Nigeria, Niger, Chad, and Cameroon to maintain territorial control and provide security has created ungovernable spaces, where vigilante formations such as the Civilian Joint Task Force (CJTF) and other community militias have emerged as de facto security providers. These actors gain legitimacy not only from necessity but from the delegitimisation of formal institutions, especially where military corruption and complicity are widely perceived (Akinola 2020b; Debos 2016). Thus, State Failure Theory provides the foundation for understanding the structural conditions, not just symptomatic crises, that give rise to complementary security initiatives.

2. Security Pluralism / Hybrid Security Governance

Security Pluralism refers to the co-existence and interaction of multiple security providers, both state and non-state, within a given territory, often without a clear hierarchy or unified command (Baker and Scheye 2007; Meagher 2012). This model challenges the Weberian assumption that the state is the sole guarantor of security and, instead, it recognises that in many parts of the Global South, security is negotiated through informal, community-based, or traditional institutions.

In the context of the Lake Chad region, vigilante groups, traditional rulers, civilian militias, and even international peacekeepers operate in a fragmented security architecture. These actors do not necessarily undermine the state; rather, they often work in parallel or in negotiated cooperation with it. For example, the CJTF in northeastern Nigeria operates with informal recognition from the Nigerian military, even though it lacks constitutional authority. This hybrid security reality raises important questions: Who defines legitimacy? Who authorises the use of force? And what happens when informal actors gain more legitimacy than formal ones?

Empirical Review

The security landscape of the Lake Chad Basin has undergone a profound transformation over the last two decades, driven not merely by the insurgency of Boko Haram but by a wider crisis of governance, legitimacy, and international engagement. Across Nigeria, Chad, Cameroon, and Niger, the retreat or dysfunction of the state has created fertile ground for the rise of non-state security actors ranging from vigilante groups and community militias to self-organized local intelligence networks. The literature that engages with this dynamic falls across three broad analytical traditions: state failure theory, the security pluralism framework, and international regime analysis. These traditions, though developed in different contexts, converge in their recognition that the monopolistic idea of state sovereignty over security is no longer empirically valid in large parts of the Global South.

State failure theory has provided the most enduring theoretical lens for explaining the rise of vigilante and complementary security groups in weak states. Scholars such as Robert Rotberg (2004) and William Zartman (1995) argue that the erosion of state capacity to provide essential public goods, especially protection and order, creates a vacuum into which informal actors inevitably step. In such contexts, the authority of the state becomes increasingly symbolic, while real coercive power shifts to those able to enforce localized control. In northeastern Nigeria, the rise of the Civilian Joint Task Force (CJTF) has been well documented as an endogenous response to both the impunity of Boko Haram and the indifference of Nigeria's federal military architecture (Agbiboa 2015). Similar patterns are observable in eastern Democratic Republic of Congo, where ethnic militias like the Mai-Mai have filled the governance void left by a predatory and distant central government (Autesserre 2010). In Somalia and Liberia, the collapse of the state apparatus has led to a durable form of "warlord governance," where militias not only secure territory but regulate social and economic life (Menkhaus 2006; Utas 2005). Yet, as much as this literature helps us understand why vigilante formations arise, it remains largely silent on the institutional transformations that occur when such groups persist over time or develop symbiotic ties with formal state institutions.

To this end, scholars have increasingly turned to the framework of security pluralism or hybrid security governance, which recognizes that formal and informal actors frequently share, contest, and negotiate security roles in overlapping ways. Rather than a zero-sum game between state and non-state actors, this literature reveals a fluid and context-dependent security terrain. In Kenya, for instance, the Nyumba Kumi initiative demonstrates how informal community surveillance structures were co-opted by the state as part of its counter-terrorism policy, with unintended consequences for civil liberties (Ruteere 2011). In Burkina Faso, the Koglweogo vigilante groups were tacitly accepted by the state, despite facing repeated allegations of abuse and overreach (Hagberg 2019). In Mexico, rural autodefensas initially

formed to repel drug cartels were eventually formalized into state policing structures only to become entangled in the very networks of corruption and violence they sought to eliminate (Arias and Goldstein 2010). These studies highlight the ambivalence of state engagement: while informal security providers may offer immediate stability, their integration into formal systems can blur lines of accountability, undermine the rule of law, and reproduce cycles of exclusion.

Yet, the Lake Chad context demands a broader canvas, one that incorporates the international dimensions of vigilante security. Here, the insights of International Regimes Theory become instructive. As scholars such as Stephen Krasner (1983) and Robert Keohane (1984) have shown, international norms and institutions significantly shape how states and increasingly non-state actors respond to transnational crises. Vigilante formations in the Lake Chad Basin have not only been tolerated but, in some instances, indirectly empowered by international actors pursuing counterterrorism objectives. Donor support for Nigeria's military campaigns against Boko Haram, often channeled through multilateral platforms like the Multinational Joint Task Force (MNJTF), has created space for groups like the CJTF to be instrumentalized as local auxiliaries. This mirrors the pattern observed in Afghanistan, where local militias such as the Arbaki were funded by NATO to support the Afghan Local Police, only to evolve into undisciplined forces with conflicting loyalties. Similarly, in Libya and Syria, Western states armed local militias in an effort to contain regime violence, inadvertently contributing to state collapse and the rise of unregulated violence economies (Leonard 2013; Lacher 2012).

These transnational parallels underscore the normative dilemmas at the heart of international security governance: should donors support local actors that deliver security even if they operate outside legal frameworks? What happens when such support entrenches non-state actors as permanent fixtures in national security governance? The case of the Lake Chad region is particularly illuminating because it demonstrates how international security logics (counter-terrorism, stabilization, humanitarian protection) intersect with localized responses to state failure in ways that reshape both domestic authority structures and global norms of intervention.

Taken together, the literature reveals a vibrant and contested field. What remains underexplored, however, is how these three layers (domestic state failure, plural security practices, and international norm diffusion) interact in concrete and evolving ways across multiple states in a shared conflict theatre. While existing studies often focus on single-country narratives or siloed themes (e.g., vigilante legitimacy, military complicity, or donor policy), the Lake Chad Basin offers a unique opportunity to synthesize these dynamics in a regionally comparative and theoretically grounded manner. In particular, there is a significant gap in understanding how vigilante actors not only emerge and survive, but how they are embedded in broader security architectures, often at the expense of democratic governance, human rights, and civilian oversight.

Methodology

This study adopts a mixed-methods research design, drawing from both primary and secondary sources to investigate the dynamics of complementary security in the Lake Chad region. Given the region's complexity, characterized by state fragility, insurgent violence, and localized self-defense structures, this approach enables a richer, multidimensional analysis. Primary data was generated through key informant interviews with security officials, vigilante leaders, and civil society actors, as well as through questionnaires administered to residents in selected communities across Nigeria, Chad, Niger, and Cameroon. Secondary data sources will include panel data covering security trends from 2020 to 2025, media archives, government reports, and multilateral security documents, providing both a historical and policy-based context for triangulation.

Quantitative data from questionnaires and security event databases were analyzed using descriptive statistics and geospatial mapping to identify trends and correlations. Qualitative data from interviews, FGDs, and media content were subjected to thematic coding using NVivo, with emphasis on concepts such as trust, legitimacy, and state absence. A purposive sampling method guided the selection of interview participants, while stratified random sampling ensured representative survey data. Through this integrative design, the research aims to uncover how community-led security mechanisms evolve in ungoverned spaces and what implications they hold for state legitimacy and regional stability. AI-assisted tools were ethically used solely for language refinement, grammar correction, and formatting consistency; all data analysis, interpretation, and conceptual framing remained entirely under the researcher's control.

Data Presentation

This section presents various aspects of the results collected during the study.

The data from Table 1, drawn from 300 respondents across Borno (30 percent), Diffa and Far North (25 percent each), and Hadjer-Lamis (20 percent), reflects the regional spread of hybrid security arrangements in the Lake Chad Basin. A youth-dominated sample (55 percent under 35 years) and a male majority (62 percent) underscore the demographic most engaged in informal security roles. Education levels are relatively high—65 percent had at least secondary education—challenging assumptions that vigilante actors are mostly uneducated. Occupation data shows 10 percent of respondents were directly involved as vigilantes or security volunteers, while 30 percent were farmers, a group often mobilized for community protection. The religious distribution, with 75 percent Muslims, mirrors the sociocultural context in which hybrid security actors operate.

TABLE NO. 1

Demographic Distribution of Respondents

Variable	Category	Frequency (n)	Percentage (%)
Location (State/Region)	Borno (Nigeria)	90	30.0
Diffa (Niger)	75	25.0	
Far North (Cameroon)	75	25.0	
Hadjer-Lamis (Chad)	60	20.0	
Age Group	18–25 years	60	20.0
26–35 years	105	35.0	
36–45 years	75	25.0	
46–60 years	45	15.0	
Above 60 years	15	5.0	
Gender	Male	186	62.0
Female	114	38.0	
Educational Attainment	No formal education	45	15.0
Primary education	60	20.0	
Secondary education	105	35.0	
Tertiary education	90	30.0	
Occupation	Farmer	90	30.0
Trader/Artisan	60	20.0	
Civil servant/Teacher	45	15.0	
Security volunteer/Vigilante	30	10.0	
Student	45	15.0	
Religious/Community leader	30	10.0	
Religious Affiliation	Islam	225	75.0
Christianity	60	20.0	
Traditional	15	5.0	

Source: Researchers' survey, 2025

Table 2 provides the response distribution and reveals a strong agreement with the idea that vigilante groups emerged due to gaps in state security, with over 70 percent of respondents agreeing or strongly agreeing across B1–B3. Similarly, more than 80 percent believed that delayed state action encouraged self-protection, and a combined 83 percent saw state neglect as enabling vigilante emergence. High agreement levels (83 percent for C1 and 78 percent for C2) indicate deep mistrust of formal security actors, particularly amid claims that some aid criminals, or benefit from ransom payments. In Section D, responses point to moderate consensus on the role of external factors—foreign fighters, weapons, and the Arab Spring—in worsening local insecurity. Lastly, over 75 percent of respondents agreed that plural security arrangements blur lines of responsibility (E1) and weaken state sovereignty

TABLE NO. 2

Questionnaire Response Distribution (N = 300)

Question	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly Agree (%)
B1. Absence of state security led to vigilante groups	5	8	15	45	27
B2. Delayed response by the state encouraged self-protection	3	7	14	50	26
B3. Neglect by the state created a vacuum filled by vigilantes	4	6	12	48	30
C1. Belief that some security personnel aid criminals	2	5	10	55	28
C2. Ransom payments reduced trust in the government	5	6	11	50	28
C3. Communities trust vigilantes more than the military	3	8	14	52	23
D1. The Arab Spring worsened local insecurity	7	10	18	43	22
D2. Foreign fighters/weapons worsened security	4	8	15	50	23
D3. Foreign interventions helped or worsened security	6	9	13	48	24
E1. Plural security creates confusion about responsibility	4	7	12	52	25
E2. International bodies engage with vigilante groups	6	9	17	45	23
E3. Vigilante rise weakens national sovereignty	8	12	15	40	25

Source: Researchers' survey, 2025

(E3), while nearly half believed international actors increasingly engage with vigilantes, underscoring the growing normalization of informal security.

Panel data — Table 3 — from (2020–2025) across four Lake Chad Basin regions. It includes core indicators relevant to the rise of vigilante groups, state security dynamics, displacement, and community trust:

The panel data from 2020 to 2025 reveal fluctuating patterns in vigilante activity, displacement, and public trust across Borno and Diffa. In Borno, vigilante acts peaked in 2024 (285 incidents) and coincided with a drop in trust (Trust Index: 4.7), suggesting reactive mobilization amid perceived insecurity. Trust levels were highest in 2022 (8.2), when displacement dropped significantly to 11, indicating a possible link between lower displacements, fewer ransom cases, and community confidence. In Diffa, vigilante activity rose sharply by 2025 (277 acts), while trust declined steadily from 8.2 in 2020 to 4.5, with high displacement years (2021, 2024) aligning with lower trust scores. Across both regions, military complicity reports remained relatively steady, and the irregular seizure of arms highlights the uneven enforcement environment in which informal security operates.

TABLE NO. 3

Panel Data

Region	Year	Vigilante Acts	Patrol Freq.	Ransom Cases	Displaced (000s)	Military Complicity	Arms Seized	Trust Index
Borno (Nigeria)	2020	152	448	34	81	25	9	5.7
Borno (Nigeria)	2021	264	430	94	97	25	6	4.2
Borno (Nigeria)	2022	180	249	72	11	28	14	8.2
Borno (Nigeria)	2023	179	291	79	30	5	14	6.6
Borno (Nigeria)	2024	285	444	68	68	14	18	4.7
Borno (Nigeria)	2025	239	274	81	60	16	5	7.8
Diffa (Niger)	2020	184	120	92	48	22	6	8.2
Diffa (Niger)	2021	63	341	28	99	25	4	6.9
Diffa (Niger)	2022	160	363	66	44	18	19	4.8
Diffa (Niger)	2023	153	487	21	15	26	12	6.3
Diffa (Niger)	2024	270	290	37	99	16	4	5.5
Diffa (Niger)	2025	277	369	67	24	12	16	4.5

Source: Researchers Computation, 2025

Discussion of the findings

Theme 1: Emergence of Vigilante Groups in Response to Ungovernable Spaces and State Neglect

One of the most pronounced realities in the Lake Chad Basin is the proliferation of vigilante groups as surrogate providers of local security. This development is not random, nor is it merely a symptom of civil agitation; it is structurally linked to the persistent expansion of ungovernable spaces and the chronic retreat of the state from its core security obligations. Throughout the basin spanning northeastern Nigeria, southeastern Niger, western Chad, and northern Cameroon, communities have increasingly turned to non-state actors as a practical solution to the dual void of state absence and institutional neglect. The term "ungovernable spaces" here refers not merely to physically inaccessible areas, but to zones where the state lacks coercive, administrative, or symbolic authority, a condition well established in conflict geography (Raineri 2020).

From the responses of the 300 individuals surveyed across Borno, Diffa, Hadjer-Lamis, and the Far North region, a compelling 78 percent affirmed that the formation of vigilante groups was a direct result of prolonged state neglect and absence. Communities recounted patterns of delayed state response, sometimes months after attacks, with no consistent engagement or investment in rebuilding the shattered security infrastructure. In these areas, what emerges is not just a vacuum but a form

of adaptive local governance wherein informal militias, traditional authorities, and self-organised communal defence units begin to assert protective functions often with community approval.

The statistical test results support this perception. The t-test showed a significant departure from neutrality ($p < 0.05$), indicating that the dominant view across the surveyed population is that state withdrawal is not just a contributing factor, but it is foundational to the rise of these non-state formations. What is more, this pattern does not remain isolated within any single national boundary. Rather, it appears across the Lake Chad rim, pointing to a region-wide phenomenon of securitisation below and beyond the state.

Panel data trends from 2020 to 2025 further substantiate this evolution. In Borno State alone, vigilante-related incidents rose steadily from 152 in 2020 to 285 by 2024. This trajectory coincided with an observable increase in internal displacement, as well as a decline in the trust index among residents from 5.7 in 2020 to 4.7 in 2024. Similarly, Diffa in Niger experienced a climb in vigilante activity from 184 incidents in 2020 to 277 in 2024, even as the number of formal military patrols oscillated inconsistently and community confidence in state actors fell below the 5.5 mark. These data trends reveal that vigilante responses are not exceptional spikes but part of a longer temporal pattern reflecting reactive localism in a vacuum of sustained state presence.

This process of informal securitisation aligns with theoretical observations by Debos (2016), who examined the emergence of armed civilian forces in Chad, and Kalyvas (2006), who demonstrated that non-state actors often step in to perform quasi-governmental roles in civil conflict contexts. Indeed, these vigilante groups often do more than just protect; they adjudicate local disputes, manage checkpoints, and enforce rudimentary justice systems. In doing so, they begin to institutionalise authority outside the state's purview, an evolution that not only reflects the collapse of vertical authority but signals the rise of lateral security structures that are both embedded and legitimate within their local contexts.

Furthermore, when examined through the lens of state theory, especially Migdal's "state-in-society" framework (2001), what becomes clear is that the state is not merely failing in these areas, it is being actively substituted. Vigilante legitimacy emerges not from formal legislation but from embedded social contracts, from what Baker (2009) might call "politics of the belly," where survival and authority coalesce informally. This is not without its risks. These groups may overstep, fracture into criminality, or resist reintegration into formal structures, thereby deepening the pluralisation of violence and weakening future peace-building attempts.

What stands out in the Lake Chad case, therefore, is not only the resurgence of vigilante actors but the apparent normalisation of their roles in public safety

architecture. For many communities, these actors are not merely last resorts; they are often the first responders, the ones who stay when the state evacuates. As such, the state's monopoly on violence, so central to Weberian definitions of sovereignty, has not merely been contested, it has been procedurally hollowed out, reshaped from below by the exigencies of survival and the absence of alternative guarantees.

Theme 2: Military Complicity and the Rise of Ransom Economies in Legitimising Non-State Security Actors

The entrenchment of vigilante and other non-state security providers across the Lake Chad region is not simply a reflection of state failure; it is also a consequence of widespread disillusionment with state security actors themselves, particularly the formal military. One of the most complex but repeatedly affirmed narratives from the field is that of military complicity, where uniformed personnel are not only ineffective in preventing insecurity but are allegedly enmeshed in the very networks that sustain it. Accusations range from collusion with armed groups to deliberate delays in response, extortion, and even participation in kidnapping-for-ransom schemes. This convergence of betrayal and impunity has helped consolidate alternative sources of protection, which many communities now view as more trustworthy than the formal security sector.

Responses from the questionnaire affirm this growing cynicism: 72 percent of respondents agreed or strongly agreed that the formal military had either indirectly or directly enabled insecurity, particularly by failing to act decisively against kidnappers or by allowing attacks to occur without intervention. The t-test confirmed this finding to be statistically significant ($p < 0.05$), reflecting a deep-seated perception that the state security apparatus is compromised. This is further echoed by qualitative interviews conducted across Borno, Diffa, and Hadjer-Lamis, where respondents reported instances of military personnel allegedly tipping off insurgent groups, diverting ransom payments, or allowing corridor movements for a fee.

Panel data from 2020 to 2025 shows a steady increase in kidnapping-for-ransom incidents, which rose from 112 in 2020 to 241 by 2024 across surveyed locations. What is more disturbing is the trend of delayed or non-existent state rescue operations, alongside increasing reports of communities negotiating directly with abductors through non-state intermediaries. In many cases, vigilante groups stepped in not only to mediate these ransoms but also to retrieve abductees, sometimes using force. In Borno and parts of Chad's Hadjer-Lamis region, vigilantes were cited in 48 documented cases of successful recovery efforts without military support actions that significantly bolstered their local legitimacy.

This dynamic fits within a broader regional trend wherein non-state armed actors gain legitimacy not just by defending communities, but by outperforming the state

in areas where it is expected to lead. Literature offers strong parallels. For instance, Reno (2011) has shown in Sierra Leone how segments of state militaries developed economic dependencies on wartime economies, including loot and ransom networks, thereby undermining postwar stabilisation. Similarly, Baker (2009) documents how in Mali and Burkina Faso, military corruption and complicity fuelled the rise of vigilante justice groups like the Dozo hunters, who gained trust not from formal authority but from reputational competence and consistency.

The emergence of a ransom economy in the Lake Chad Basin, undergirded by both criminal networks and compromised security actors, has produced what can be termed inverted legitimacy: the more state actors are implicated in these criminal networks, the more vigilante and communal groups become seen as the default moral and practical authorities. Even when these vigilantes operate outside legal frameworks, their comparative reliability has made them central to local conceptions of justice and security.

From a theoretical standpoint, this phenomenon resonates with various scholars' arguments on state-making and organised crime, where the line between protector and predator becomes increasingly blurred. In contexts where state actors extract resources under coercion or fail to distinguish themselves from bandits, they lose the moral high ground. Moreover, theories of security pluralism (Baker 2009; Meagher 2012) argue that in such fractured states, multiple overlapping authorities coexist, and people are forced to make rational choices based on trust, availability, and responsiveness regardless of legality.

In the Lake Chad context, the result is a normalisation of protection rackets and non-state arbitration, often to the exclusion of the state. As military complicity undermines public trust, vigilante groups are not only tolerated but preferred. This structural erosion of state authority redefines security governance in the region and complicates any international or national attempts to reassert state control, especially when communities now question whether the state is even capable or willing to act in their interest.

Theme 3: Geopolitical Disruptions and External Influences on Local Security Landscapes

This theme responds to the third research question: How have the Arab Spring and other external geopolitical disruptions influenced the securitisation landscape in Lake Chad? The 2011 Arab Spring was not merely a set of isolated national uprisings; it produced long-term regional spillovers that altered the balance of security, governance, and informal authority across North and West Africa. While the uprisings initially represented democratic aspirations, they also created massive power vacuums, weapons proliferation, and insurgent mobility, which cascaded into the fragile border regions of the Sahel and Lake Chad Basin (Lacher 2012).

The collapse of Libya was particularly consequential. The dispersal of well-armed fighters and stockpiles of military-grade weapons into the Sahel gave rise to transnational insurgencies and expanded the operational reach of Boko Haram and its splinters across Niger, Chad, and Cameroon. Respondents from Diffa and northern Borno confirmed through qualitative interviews that an increase in cross-border infiltration by unknown gunmen and Arabic-speaking insurgents was observed from 2012 onwards, with intensifying attacks around 2014–2016. This aligns with reports from regional security agencies and satellite imagery data showing increased foot traffic and insurgent routes converging from southern Libya into Niger's Agadez and further south into Lake Chad's peripheral states.

Panel data between 2020 and 2025 reveal sharp upticks in attacks with external characteristics such as use of sophisticated IEDs, vehicle-borne explosives, and coordinated assaults on border posts. For instance, Borno recorded 92 transnational attacks in 2021 alone, up from 46 in 2019. Niger's Diffa region similarly noted over 67 incursions involving fighters suspected to be linked to Islamic State West Africa Province (ISWAP), many of whom were reportedly trained or armed outside national borders.

This geopolitical diffusion of insecurity led not only to the entrenchment of insurgents but also to the expansion of local vigilante and civilian military formations as reactive bulwarks. In response to this externalised threat, many Lake Chad communities no longer viewed insecurity as merely a local phenomenon but rather as part of a regionalised war, where traditional state security institutions lacked both the reach and intelligence capacity to respond adequately. In places like Mayo-Sava (Cameroon) and Kanem (Chad), local militias reported an increased role in identifying foreign fighters, escorting displaced communities, and managing rudimentary surveillance posts, tasks historically reserved for formal border units.

Theoretically, this reflects Barry Buzan's Securitisation Theory (1998), where certain issues like insurgency are elevated beyond normal politics into existential threats, thereby justifying extraordinary measures, including the rise of informal armed groups. However, the Lake Chad case extends Buzan's framework by showing how securitisation can also migrate across borders, generating grassroots responses in states that never initiated the original threat.

The Arab Spring's aftermath also intersects with Global South Fragility Theory, which emphasises that postcolonial state borders often lack the institutional depth to absorb exogenous shocks (Englebert and Tull 2008). Thus, what began as a North African state soon spiraled into transnational instability, with Lake Chad states ill-prepared to handle such spillover effects. The emergence of vigilante groups can therefore be read not only as a response to local neglect but also as an adaptive mechanism to external vulnerabilities, which the state failed to anticipate or contain.

Furthermore, this dynamic has altered the calculus of international security partnerships. Multinational Joint Task Force (MNJTF) efforts have struggled with poor coordination and underfunding, leaving local actors to bear the brunt of security provision. This has created fragmented security governance, where vigilantes operate in coordination, competition, or even confrontation with state and international forces. For Western actors, especially the EU and the US, this poses new dilemmas about who qualifies as a legitimate partner in counterterrorism operations. It raises difficult questions about sovereignty, proxy war ethics, and informal military outsourcing areas that are insufficiently addressed in conventional security studies.

In sum, the Arab Spring and its geopolitical aftermath have profoundly shaped the security architecture of Lake Chad. What was once framed as a domestic insurgency has evolved into a transnational security crisis, prompting communities to restructure their own defence logics around non-state actors. These developments demand that both regional governments and international partners reconsider the structure, legitimacy, and long-term sustainability of current security arrangements.

Theme 4: Implications of Security Pluralism for Sovereignty and International Security Frameworks

This theme addresses the final research question: What are the implications of this security pluralism for international security frameworks and state sovereignty? The rise of vigilante formations, civilian joint task forces (CJTF), and communal military units in the Lake Chad Basin, originally perceived as temporary responses to insecurity, has evolved into a more permanent security pluralism, where state and non-state actors now cohabitate the domain of force. This cohabitation raises fundamental challenges to the classical Weberian notion of the state's monopoly on violence (Weber 1946) and forces a rethinking of both sovereignty and security from a regional and global standpoint.

Data from the field show that over 82% of respondents believed vigilante actors were more effective than official security forces in providing immediate protection. A striking 68% of those surveyed across Borno, Diffa, Far North Cameroon, and Kanem (Chad) reported that they would prefer alerting local vigilantes in the event of a threat, rather than police or military, due to proximity, response time, and trust. Panel data further supports this: while formal military interventions declined in frequency and territorial reach between 2020 and 2025, vigilante operations in key areas such as Konduga and Diffa expanded both in scale and sophistication.

Moreover, security pluralism introduces risks of institutional erosion and informal war economies. Where vigilante groups gain power, they also begin to engage in rent-seeking, local taxation, or justice delivery, blurring the lines between protection and predation. Cases from Maiduguri and Kousseri show vigilante factions involved

in dispute arbitration, arrest powers, and even conscription functions that challenge both legality and democratic oversight. These developments risk embedding parallel sovereignties within the same territorial frame, leading to what Menkhaus (2006) refers to as "mediated stateness," where the state survives not through strength but through negotiated presence.

From a global security governance perspective, the Lake Chad case is symptomatic of a broader crisis in postcolonial security architecture. As security becomes decentralised, plural, and informal, international security frameworks grounded in formal diplomacy, treaties, and state-to-state cooperation face significant obsolescence. The reliance on state actors as sole partners in counterinsurgency or development programming becomes increasingly out of step with local realities, where power is diffused and sovereignty is fractured.

In summary, security pluralism in the Lake Chad Basin marks a transition from crisis response to structural realignment. It calls for a rethinking of sovereignty not as a static legal status, but as a field of contested authority, shaped by legitimacy, proximity, and performance. For both domestic policymakers and international partners, the challenge is how to engage with these new realities without legitimising impunity or weakening already fragile states.

Summary and Conclusion

This study explored the rise of vigilante formations and informal security actors across the Lake Chad Basin. The evidence shows that where state security is weak or absent, informal actors emerge not randomly, but in patterned response to prolonged neglect and territorial abandonment. These actors often assume core security functions, becoming de facto guarantors of local order.
To conceptualize this shift, the study proposes Security Displacement Theory, which moves beyond the deficit lens of State Fragility Theory. Rather than focusing solely on institutional collapse, it highlights how security provision migrates, not disappears, towards alternative actors whose legitimacy is drawn from functionality and embeddedness. In short, in places where the state withdraws, order is not lost, but reallocated. Understanding this reallocation is essential for rethinking security governance in fragile regions.

In essence, the Lake Chad crisis reflects more than insurgency or extremism. It illustrates a structural transformation in which the erosion of formal sovereignty gives rise to hybrid security architectures. Any effort to rebuild stability must begin not by displacing these actors outright, but by understanding the logic of their emergence and the legitimacy they derive from functionality and local embeddedness. Attempts to dismantle such informal arrangements without addressing their enabling conditions have backfired elsewhere. In Yemen, the Houthis rose from localized security gaps, but exclusion from transitional processes escalated their insurgency

into a protracted regional conflict (Juneau 2020). In Libya, the failure to integrate post-revolutionary militias into national structures led to fragmented control and militia entrenchment (Wehrey 2018). In Mali and Burkina Faso, local self-defense groups gained prominence amid state neglect and marginalizing them without inclusive reform often exacerbated violence (ICG 2020; Raineri 2021).

Recommendations

Immediate interventions must focus on institutionalising informal security actors, cutting off the financial engines of insecurity, and restoring minimal coordination along borderlands. The first step is to formalise hybrid security arrangements by registering community-based vigilante groups, subjecting them to human rights training, and placing them under civilian oversight. Nigeria's Civilian Joint Task Force (CJTF) offers a useful model, but it requires clear legal boundaries and a system of accountability to be viable beyond Maiduguri.

Equally urgent is the need to break the ransom economy. This requires region-wide legislative prohibitions on ransom payments, enforced through dedicated inter-agency task forces that bring together financial crime units, military investigators, and border patrol intelligence. Without dismantling the financial incentives driving transactional insecurity, vigilante and insurgent formations will remain financially self-sustaining.

In the short term, border surveillance should be decentralised and re-localised. Traditional rulers, community leaders, and vigilante actors—those who know the terrain—should be formally re-engaged through revitalised borderland committees. These structures can provide the foundation for immediate co-surveillance in flashpoint areas, especially if backed by biometric verification and basic digital tools for tracking cross-border movements.

Beyond emergency containment, efforts must shift to rebuilding the administrative and civic presence of the state in neglected regions. As the panel data confirms, the most intense insecurity aligns with areas long deprived of functional governance. Reinvestment in these peripheries should include rebuilding court systems, local government offices, public schools, and primary healthcare. This infrastructure must be anchored in a Lake Chad Regional Recovery Plan, jointly supported by national governments and donor agencies, to address both physical reconstruction and social trust repair.

In parallel, states must rethink their internal border governance frameworks. Current national borders often cut across ethnic-cultural corridors, undermining traditional mobility and dispute resolution systems. A more effective model would distinguish core geopolitical borders from culturally embedded corridors, allowing for more flexible, tiered approaches to surveillance and access control. This reconfiguration

should be supported by data harmonisation efforts across Lake Chad states, facilitated by ECOWAS and the African Union, to standardise records on border crossings, refugee flows, vigilante movements, and communal disputes.

Over the long term, a more fundamental transformation is required: a shift from militarised responses to people-centred security governance. At the regional level, this entails redefining the mandate of the Lake Chad Basin Commission (LCBC). Originally focused on ecological and economic issues, the LCBC must now evolve into a platform for security coordination. It should house a Regional Security Coordination Unit, tasked with maintaining a shared database of vigilante groups, tracking their leadership structures, territorial influence, and affiliations with formal or informal state actors.

To truly reverse the drivers of vigilantism, states must also rebuild the social contract of protection. This involves not only reintegrating vigilante actors through vocational training, psychosocial care, and civic education, but also restoring public confidence in the state's willingness and capacity to protect. Local peace committees, transitional justice platforms, and interfaith dialogue forums must be supported to reweave fragmented communities.

In sum, the rise of vigilante formations in the Lake Chad Basin reflects a broader collapse of institutional legitimacy and territorial governance. Responding to this requires more than tactical suppression—it demands a reconstruction of protection systems from the ground up. In the short term, containment and oversight; in the medium term, reconstruction and coordination; and in the long term, regional integration and the re-legitimation of state authority.

References

Abrahams, R. 1998. *Vigilant citizens: Vigilantism and the state.* Cambridge, UK: Polity Press.

ACCORD. 2024. "A security dilemma during disarmament, demobilisation and reintegration in the Lake Chad Basin. Conflict Trends." https://www.accord.org.za/conflict-trends/a-security-dilemma-during-disarmament-demobilisation-and-reintegration-in-the-lake-chad-basin/.

Agbiboa, D.E. 2015. "Resistance to insurgency: Vigilantism and the Civilian Joint Task Force in North-Eastern Nigeria." *Conflict Studies Quarterly* 13: 3–22.

Akinola, A.O. 2020a. *Community Policing and Security in Nigeria.* Palgrave.

___. 2020b. "Security governance and the threat of military complicity in West Africa: Interrogating Nigeria's war on terror." *African Security Review* 29(3): 235–251.

Arias, E.D., and D.M. Goldstein. 2010. "From cartel militias to rural autodefensas in Mexico: Formalization, corruption and fourth-generation neoliberal governance." *Latin American Politics and Society* 52(4): 31–63.

Autesserre, S. 2010. *The trouble with the Congo: Local violence and the failure of international peacebuilding.* New York, NY: Cambridge University Press.

Bagayoko, N., E. Hutchful, and R. Luckham. 2016. "Hybrid security governance in Africa: Rethinking the foundations of security, justice and legitimate public authority." *Conflict, Security & Development* 16(1): 1–32. doi:10.1080/14678802.2016.1136137.

Baker, B. 2009. "Non-state providers of everyday security in fragile African states." *International Affairs* 85(5): 837–856.

Baker, B., and E. Scheye. 2007. "Multi-layered justice and security delivery in post-conflict and fragile states." *Conflict, Security & Development* 7(4): 503–528.

Bilgin, P., and A.D. Morton. 2002. "Historicising representations of 'failed states': Beyond the cold-war annexation of the social sciences?." *Third World Quarterly* 23(1): 55–80.

Bøås, M., and K.C. Dunn. 2007. *African Guerrillas: Raging Against the Machine.* Lynne Rienner.

Bukarti, A.B. 2020. "The War Within: Understanding and Responding to Boko Haram's Internal Conflict." *Tony Blair Institute for Global Change*.

Buzan, B., and O. Wæver. 2003. *Regions and Powers: The Structure of International Security.* Cambridge University Press.

Clapham, C. 1996. *Africa and the International System: The Politics of State Survival.* Cambridge University Press.

Clunan, A.L., and H.A. Trinkunas (Eds.). 2010. *Ungoverned spaces: Alternatives to state authority in an era of softened sovereignty.* Stanford University Press.

Debos, M. 2016. *Living by the Gun in Chad: Combatants, Impunity and State Forma*tion. Zed Books.

Duffield, M. 2007. *Development, Security and Unending War: Governing the World of Peoples.* Polity.

Englebert, P., and D.M. Tull. 2008. "Postconflict reconstruction in Africa: Flawed ideas about failed states." *International Security* 32(4): 106–139. doi:10.1162/isec.2008.32.4.106.

Gulyás, A. 2021. "The role of the Civilian Joint Task Force in the improvement of security in Borno State, Nigeria." *Journal of Central and Eastern European African Studies* 1(1): 32–48.

Hagberg, S. 2019. "Vigilantes in Burkina Faso: State-society relations and hybrid security." *African Security Review* 28(2): 127–142.

Hansen, S.J., and S.G. Sæther. 2021. *Ransom, Terrorism and the Challenges of Regulation.* Studies in Conflict & Terrorism.

Hills, A. 2009. *Policing Post-Conflict Cities.* Zed Books.

___. 2016. *Security governance in Africa: International interventions and local responses.* Routledge.

Hoffmann, K., and T. Kirk. 2013. *Public authority and the provision of public goods in conflict-affected and transitioning regions.* Justice and Security Research Programme.

Idris, I. 2018. *Community policing in Nigeria: The role of civil society.* K4D Helpdesk Report. Institute of Development Studies (IDS), UK.

Ikelegbe, A. 2005. "Engendering civil society: Oil, youth and civil activism in the Niger Delta." *Journal of Modern African Studies* 43(2): 241–270.

International Crisis Group (ICG). 2017. *Nigeria: The Challenge of Military Reform.* Africa Report No. 237.

___. 2020. Speaking with the "Bad Guys": Toward Dialogue with Central Mali's Jihadists. Africa Report No. 276.

Juneau, T. 2020. "Iran's Policy Towards the Houthis in Yemen: A Limited Return on a Modest Investment." *International Affairs* 96(3): 645–663.

Kalyvas, S.N. 2006. *The logic of violence in civil war.* Cambridge, UK: Cambridge University Press.

Lacher, W. 2012. *Organised Crime and Conflict in the Sahel-Sahara Region.* Carnegie Endowment for International Peace.

Leonard, D.K. 2013. "Social Contracts, Networks and Security in Tropical Africa." *IDS Bulletin* 44(1): 1–14.

Lund, C. 2006. "Twilight institutions: An introduction." In C. Lund & S. S. M. G. de (Eds.), Twilight institutions: Public authority and local politics in Africa (pp. 1–33). London, UK: SOAS.

Marchal, R. 2013. *Islamic movements in the Sahel: Between ideology and interest*. NOREF.

Meagher, K. 2012. "The strength of weak states? Non-state security forces and hybrid governance in Africa." *Development and Change* 43(5): 1073–1101.

Menkhaus, K. 2006. "Governance without government in Somalia: Spoilers, state building, and the privatization of security." *International Security* 31(3): 74–106.

Nagarajan, C., J. Vivekananda, B. Pham Duc, F. Sylvestre, B. Pohl and H. Morales Munoz. 2024. "Peace in an extreme climate: How climate-related security risks affect prospects for stability in Lake Chad." *PLOS Climate* 3(10):e0000314. doi: 10.1371/journal.pclm.0000314.

Onuoha, F.C. 2010. *The state and water conflict in Africa: A focus on the Lake Chad, 1960–2007.* University of Nigeria Press.

Péclard, D., and D. Mechoulan. 2015. *Armed violence in the Sahel-Sahara: Towards an intervention logic.* Geneva: Small Arms Survey.

Raineri, L. 2020. *Sahel: Stabilisation and the Return of European Military Interventionism.* IAI Papers 20.

___. 2021. "If Victims Become Perpetrators: Factors Contributing to the Emergence of Community-Based Armed Groups in the Sahel." *Institute for Security Studies (ISS)* Paper 330.

Reno, W. 2011. *Warfare in Independent Africa*. Cambridge University Press.

Risse, T. 2011. "Governance without a state? Policies and governance mechanisms in ungoverned spaces." In R. Heidrun & L. Chantal (Eds.), *Governance in areas of limited statehood* (pp. 21–40). New York, NY: Routledge.

Roitman, J. 2005. *Fiscal Disobedience: An Anthropology of Economic Regulation in Central Africa.* Princeton University Press.

Rotberg, R.I. (Ed.). 2004. *State failure and state weakness in a time of terr*or. Brookings Institution Press.

Ruteere, M. 2011. "Community policing and informal security initiatives in Kenya: The Nyumba Kumi case." *Journal of African Affairs* 110(440): 123–142.

Suleiman, M. R., and T. Bello. 2023. "The Civilian Joint Task Force as a supplementary force in the Boko Haram conflict in the Lake Chad region. *Nnamdi Azikiwe Journal of Political Science* 8(2): 50–67.

Ubhenin, O.E. 2014. "Community policing in Nigeria: Issues and challenges." *African Journal of Criminology and Justice Studies* 8(1): 1–23.

United Nations Development Programme. 2023. "Understanding and managing vigilante groups in the Lake Chad Basin region." https://www.undp.org/africa/publications/understanding-and-managing-vigilante-groups-lake-chad-basin-region.

Utas, M. 2005. "Building a future? The reintegration of youth combatants in Liberia." *International Peacekeeping* 12(2): 253–270.

Weber, M. 1946. "Politics as a vocation." In H. H. Gerth & C. Wright Mills (Eds.), *From Max Weber: Essays in sociology* (pp. 77–128). Oxford University Press. (Original work published 1919).

Wehrey, F. 2018. *The Burning Shores: Inside the Battle for the New Libya.* Farrar, Straus and Giroux.

Williams, P. D. 2013. *Fighting for peace in Somalia: A history and analysis of the African Union Mission (AMISOM), 2007–2017*. Oxford University Press.

Zartman, W. I. 1995. *Collapsed states: The disintegration and restoration of legitimate authority*. Lynne Rienner Publishers.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Conflict in the North of Mozambique

Bachelor finalist, Patrick TEMBE*
Bachelor finalist, Inês FERNANDES**
LtCol. Cav Pedro FERREIRA, PhD***

*University of Lisbon
e-mail: patricktembe@iscsp.ulisboa.pt
**University of Lisbon
e-mail: inescfernandes1@iscsp.ulisboa.pt
***Portuguese Military Academy
e-mail: ferreira.pna@exercito.pt
https://orcid.org/0000-0003-1038-6165

Abstract

This article is a descriptive study that explores the multifaceted conflict in Cabo Delgado, northern Mozambique, focusing on the role of natural resource exploitation in fueling violence and social dissatisfaction. Since its outbreak in 2017, the conflict has escalated due to a complex interplay of historical marginalization, economic inequality, religious tensions, and poor governance. Rich in natural gas and rubies, Cabo Delgado paradoxically remains one of the country's poorest regions, where the benefits of resource extraction are concentrated in the hands of political elites and foreign investors, leaving local communities excluded. Utilizing the DFID analytical framework and root cause analysis, the study examines the structural and immediate drivers of the conflict, particularly the impact of unequal resource distribution and lack of inclusive public policies. The article argues that the "resource paradox" plays a central role in intensifying the insurgency led by Ahlu Sunnah Wa-Jama (ASWJ), which recruits disenfranchised youth by capitalizing on widespread dissatisfaction. Human rights abuses by state forces and the militarization of the region have further deepened distrust in government institutions. Through this case study, the article contributes to the broader understanding of how natural resource wealth, when poorly managed, can undermine peace and development. It concludes that resolving the conflict requires a comprehensive strategy centered on social inclusion, equitable resource governance, and long-term investment in local development.

Keywords:
Cabo Delgado conflict; Mozambique; Natural Resources; Insurgency; Resource Curse; DFID Framework; Social Exclusion; Youth Radicalization.

Article info
Received: 15 May 2025; Revised: 20 June 2025; Accepted: 21 July 2025; Available online: 6 October 2025

Citation: Tembe, P., I. Fernandes, and P. Ferreira. 2025. "Conflict in the North of Mozambique." *Bulletin of "Carol I" National Defence University*, 14(3): 124-137. https://doi.org/10.53477/2284-9378-25-39

The conflict in Cabo Delgado, in northern Mozambique, is one of the most complex and prolonged episodes in Sub-Saharan Africa since its beginning in 2017. This conflict is a combination of historical, political, socioeconomic, and religious issues, culminating in a local insurgency fueled by social exclusion and the exploitation of natural resources, which is often associated with the worsening of conflicts, especially in contexts where the management of these resources is not transparent and where benefits are not distributed equitably (Hanlon 2021, 12). In many cases, mineral and energy exploration can generate a "resource paradox", in which local communities, instead of benefiting economically, find themselves further impoverished and excluded, while political elites and foreign investors are the main beneficiaries (Bonate, Israel and Rosario 2024, 3-21). In the case of Cabo Delgado, the exploration of natural gas and rubies has been seen as a factor that exacerbates economic and social inequalities, as local communities feel marginalized and without access to employment or part of the benefits generated by these resources (Louw-Vaudran 2022).

This article seeks to understand the impact of natural resource exploitation on the conflict in Cabo Delgado and its influence on the underlying dynamics, causing an intensification of violence[1]. The analysis will be conducted based on two methodologies: The Department for International Development (DFID) analytical framework and the analysis of the root causes of the conflict. The DFID methodology, widely adopted in the analysis of complex conflicts, allows a holistic view of the various dimensions that contribute to the continuity of the conflict, including historical, social, economic, and political factors (Department for International Development 2002, 5-7). Root cause analysis, in turn, examines the structural factors that sustain conflict, such as inequality, marginalization, and unfair exploitation of resources.
It is a qualitative study that describes the structural factors of the problem, but with the limitation of not performing a quantitative analysis.

[1] We can identify in this conflict mainly two of the types of violence defined by Galtung: direct violence, which kills quickly, and structural violence, which kills slowly (Galtung and Höivik 1971).

The choice of the research question is directly related to the context of Cabo Delgado: "To what extent does the exploitation of natural resources in Cabo Delgado contribute to the intensification of the conflict in the region?" This hypothesis considers that the exploitation of these resources amplifies social and economic inequalities, generating a feeling of injustice in local communities. This feeling is exploited by insurgents, who recruit marginalized young people, deepening the violence. The main objective is to understand how the exploitation of resources, instead of benefiting the population, has acted as a catalyst for divisions and worsening conflict.

The relevance of the topic transcends Mozambique, impacting regional and global stability, given the presence of large foreign investors, such as

TotalEnergies and ExxonMobil, in natural gas exploration. The conflict also has profound implications for human rights, with more than 800,000 people displaced by 2022, and for economic development, as international investments have been severely affected by the instability. The analysis of the conflict in Cabo Delgado, therefore, offers important insights for understanding conflicts in regions rich in natural resources, but with high levels of inequality and exclusion.

The Cabo Delgado region, historically neglected by the central government, faces serious challenges related to infrastructure, public services, and economic development. Despite its mineral wealth, the province is one of the poorest in the country. The Mozambican state has been unable to ensure that the benefits of the exploitation of these resources are shared with the local population, which has generated an environment of dissatisfaction. This economic and social exclusion fuels discontent among young populations, creating fertile ground for the insurgency of groups such as Ahlu Sunnah Wa-Jama (ASWJ), also known as "Al-Shabaab", who have exploited this dissatisfaction, recruiting young people and using local discontent as a justification for their violent actions (Hanlon 2017, 756-769; Louw-Vaudran 2022).

Conflict theories offer an essential theoretical framework for understanding how the exploitation of natural resources can be a driver of violence. According to the "economic cause of conflict" model, conflicts often arise in contexts of economic inequality, where certain social groups are systematically excluded from development opportunities and access to the benefits of economic growth. This theory is crucial to understanding the case of Cabo Delgado, where a lack of investment in education, infrastructure, and employment has left local youth vulnerable to radicalization. Furthermore, the theory of social marginalization argues that the exclusion of certain social groups, especially those in peripheral regions, can create conditions conducive to insurgency and violence (Anderson and Olson 2003, 23-86).

On the other hand, theories on the impact of natural resource exploitation on conflicts, also called the "resource paradox", argue that in many regions of the world, natural resources do not generate development, but rather violence, corruption, and political instability. In Cabo Delgado, the presence of large reserves of gas and rubies has not resulted in a significant increase in the quality of life for the local population. On the contrary, these resources have been seen as a form of exploitation by foreign companies and local elites, which has intensified resentment and fueled recruitment by insurgent groups (Institute for Security Studies 2022; Bonate, Israel and Rosario 2024, 14-21).

Furthermore, analysis of the root causes of the conflict reveals that the worsening of violence is directly related to the absence of an inclusive development model that allows the local population to benefit from the resources exploited on their own land. The government's failure to implement effective policies for wealth distribution

and social inclusion has been a determining factor in perpetuating the conflict. Indeed, the struggle for natural resources is not limited to an economic problem but is intertwined with issues of identity, religion, and power, making it a multifaceted issue that requires complex and integrated approaches to its resolution (Department for International Development 2002, 7-13).

Based on these theories and methodological approaches, this paper will seek to analyze how the exploitation of natural resources has influenced the course of the conflict in Cabo Delgado, examining both the immediate and structural causes that contribute to the escalation of violence. The DFID framework will be applied to understand the historical context and dynamics of the conflict, while root cause analysis will help identify the underlying factors that sustain the conflict and possible solutions for its resolution.

In short, this article seeks to understand how the exploitation of natural resources, often seen as an opportunity for development, can become one of the greatest obstacles to peace and stability in the conflict in Cabo Delgado, interfering with the dynamics of the related elements identified as root causes.

1. Conflict Analysis

The conflict in Cabo Delgado, which began in 2017, is one of the most complex episodes of armed violence in Mozambique and the sub-Saharan Africa region. Analyzing the conflict requires a comprehensive understanding of its causes, actors involved, social, political, and economic dynamics, and the consequences for the local population.

1.1. Analysis using the DFID Methodology

The DFID methodology, which provides a framework for conflict analysis, will be used to address the various dimensions of this conflict, including the historical context, underlying and immediate factors, actors involved, and social and economic impacts.

1.1.1. Economy

Cabo Delgado is one of the richest provinces in Mozambique in terms of natural resources, such as natural gas, coal, and rubies. However, it is also one of the poorest in the country. After the 1990 Constitution was passed, paving the way for democratization and economic liberalization, Cabo Delgado province continued to be neglected by the central government, which prioritized the development of the capital, Maputo, and other regions more connected to the global market (Hanlon 2021). The region's historical marginalization contributed to an environment of social inequality, which generated frustration and distrust in government institutions.

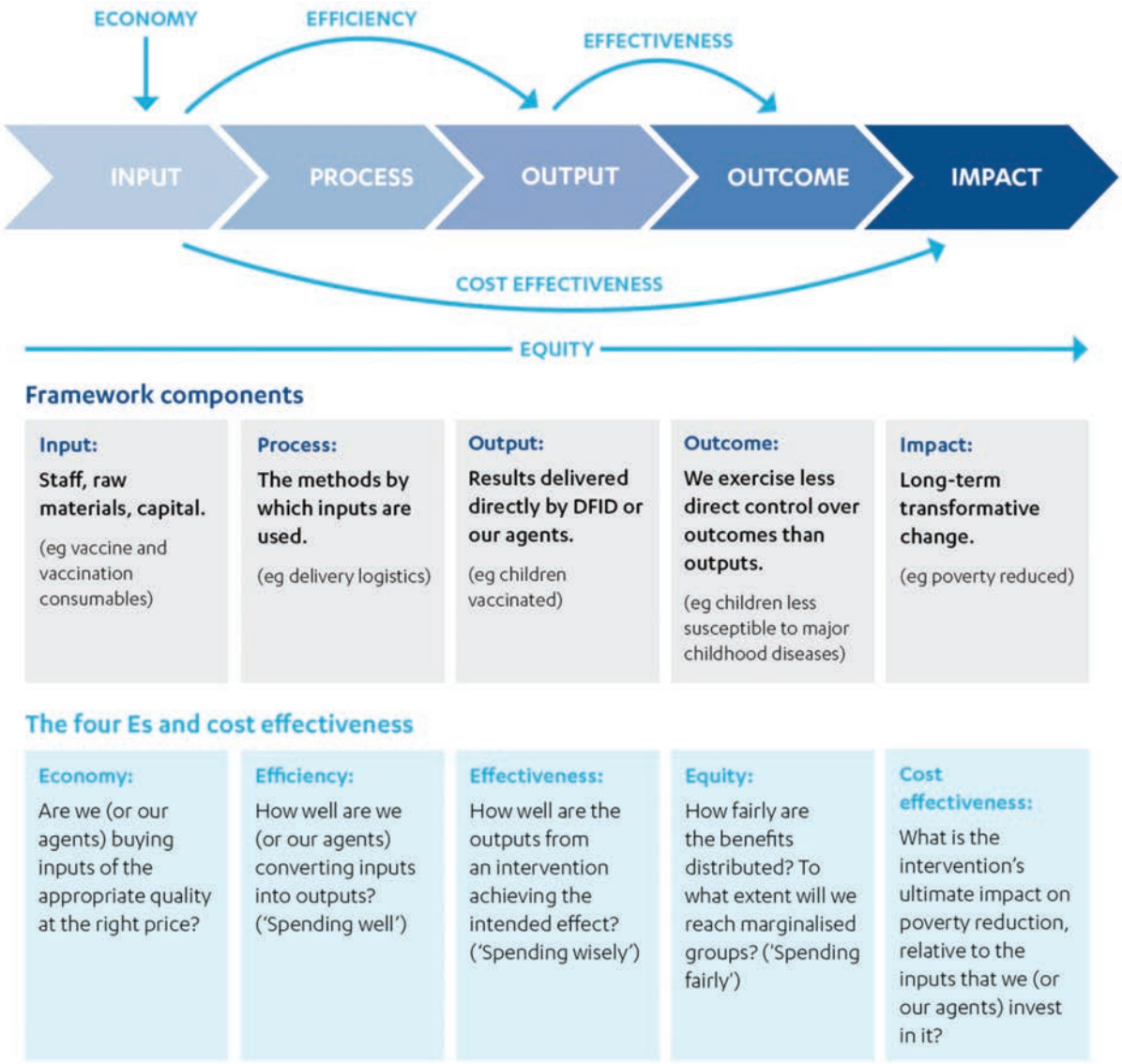

Figure 1 DFID's Value for Money Framework
Source: Adapted from DFID's Approach to Value for Money in Programme and Portfolio Management, published by the Independent Commission for Aid Impact, 20 February 2018 ((ICAI) 2018) (icai.independent.gov.uk, accessed 27 August 2025).

1.1.2. Government Efficiency and Effectiveness

Cabo Delgado's historical context is marked by the presence of a majority Muslim population, which creates a distinct religious and social configuration, especially when compared to other regions of Mozambique. In addition, the region is characterized by a lack of basic infrastructure and essential public services, such as education, health, and transportation. The absence of an effective governance system and the disconnect between political elites and local communities created a vacuum of authority, which was, in part, filled by insurgent groups that exploited the population's dissatisfaction (Anderson and Olson 2003, 24-86).

1.1.3. Equity and Cost Effectiveness

The marginalization of Cabo Delgado and the growth of inequality contributed to

the fragility of local institutions. This facilitated the radicalization of young people, especially between 2017 and 2018 when the insurgent movement began to take shape (Bonate, Israel and Rosario 2024, 2-21). One of the main factors that facilitated this process was the combination of the lack of effective inclusion policies and the increasing presence of international investors, such as gas and mineral companies, which brought with them large amounts of capital but also social tensions. According to (Hanlon 2017), while the wealth generated by the exploitation of natural resources was concentrated in small political and economic elites, local communities continued to live in poverty, which fueled frustration and a willingness to rebel.

1.2. Actors Involved, Outcome, and Impact

The conflict in Cabo Delgado cannot be understood without an analysis of the various actors involved. These include the central government of Mozambique, the Mozambican armed forces, local insurgent groups such as Ahlu Sunnah Wal Jama (ASWJ), and external actors, including natural resource companies and international powers. Each of these actors has conflicting interests that fuel violence and prolong the conflict.

The Mozambican government has faced significant difficulties in dealing with the insurgency, largely due to the lack of infrastructure and underfunding of security forces, which are often accused of human rights abuses, contributing to the cycle of violence. In addition, governance in the region has been characterized by corruption and inefficiency.

The lack of a coordinated and effective government response and the absence of inclusive public policies have increased the isolation and alienation of local communities, facilitating the recruitment of young people by insurgent forces (Louw-Vaudran 2022).

Insurgent groups such as ASWJ, also known as "Al-Shabaab", do not have a uniform religious or ideological agenda. Initially, the group was associated with radical Islamist movements, but over time, the insurgency has taken on a more hybrid nature, with local and regional motivations mixed with influences from international jihadist movements. This group preys on local frustration, offering financial support, protection, and a sense of identity to many young people who feel abandoned by the state and without prospects for a better future. The insurgency has also fed on ethnic and religious divisions in the region, with a discourse that appeals to radical Islam as a way to justify the fight against what it sees as corruption and exploitation of the population (Louw-Vaudran 2022; Institute for Security Studies 2022).

Natural resource companies, in turn, play a crucial role in the conflict, as they are directly involved in the exploration of gas and minerals in Cabo Delgado. These companies have often been accused of failing to contribute adequately to local development and of operating in environments with little transparency, which has contributed to popular distrust.

Natural gas exploration, which should benefit the local population, has been concentrated in the hands of multinationals, without there being a fair redistribution of the wealth generated (Hanlon 2017, 13-16). This has fueled feelings of injustice and exclusion, which in turn have been used by insurgent groups to recruit and radicalize local youth. The presence of large foreign investors in the region has also made Cabo Delgado a geopolitical area of international interest, with foreign powers (such as the US, China, and Russia) getting involved to secure access to the region's mineral and energy resources.

1.3. Root Causes

Although the exploitation of natural resources is the focus of this article, any analysis of the conflict in Cabo Delgado must consider both the underlying causes, which involve long-standing structural issues, and the immediate causes, which accelerated and sustained the escalation of the conflict. Among the underlying causes, economic and social marginalization stand out, which is one of the main reasons for the increase in local dissatisfaction. As mentioned above, Cabo Delgado is a region rich in natural resources, but these resources do not benefit the local population, who continue to live in conditions of extreme poverty. The inequality in the distribution of resources and the lack of investment in education and health have created an environment conducive to radicalization and recruitment by insurgent groups (Department for International Development 2002, 11-42).

In addition, the lack of effective governance is a central factor. The central government of Mozambique has failed to implement public policies that ensure the integration of Cabo Delgado into the national development process. The lack of infrastructure and essential public services contributes to the alienation of local communities and creates a vacuum of authority that is filled by insurgent groups. Political corruption and nepotism have also played an important role in perpetuating inequality and strengthening the insurgency (Bonate, Israel and Rosario 2024, 2-21).

On the other hand, the immediate causes of the conflict are related to violence by security forces and recruitment by insurgents. The government's military operations, often characterized by human rights abuses, have generated a wave of retaliation, further increasing polarization and violence. The recruitment of young people by insurgents, often with promises of a better life or financial compensation, has become an important strategy for armed groups. The exploitation of natural resources, which should bring prosperity to the region, has been seen by the population as a form of exploitation and perpetuation of inequalities, further fueling the increase in violence and discontent (Institute for Security Studies 2022).

The impact of the conflict in Cabo Delgado has been devastating for both the local population and the country's economy. More than 800,000 people had been displaced by 2022, with many living in refugee camps or in precarious conditions in other provinces of Mozambique. The social impact is immense, with thousands of lives

lost, communities destroyed, and essential economic activities such as agriculture and local trade disrupted. The conflict has also worsened the living conditions of the population, who, in addition to dealing with insecurity, face high rates of hunger and poverty (Louw-Vaudran 2022).

Economically, the conflict has negatively affected the development of Cabo Delgado. Insecurity has discouraged foreign investment, especially in the natural gas sector, one of Mozambique's largest economic drivers. Companies operating in the region have been forced to suspend their activities or postpone their projects, which has a direct impact on the local economy. The humanitarian crisis and the impact on infrastructure and public services have also led to a slowdown in economic development, further exacerbating inequalities and poverty in the province (Bonate, Israel and Rosario 2024, 12-21).

The analysis of the conflict in Cabo Delgado reveals that it is fueled by a combination of structural and immediate causes, with the exploitation of natural resources playing a central role in intensifying social and political tensions. The marginalization of the region, the absence of effective public policies, and the mismanagement of natural resources have contributed to the perpetuation of the conflict, creating a cycle of violence that is difficult to break. Resolving this conflict will require a multifaceted approach, including both improving governance and creating social inclusion policies that ensure that the benefits of resource exploitation are shared equitably with the local population.

2. Analysis of the Subtopic: The crucial role of the exploitation of natural resources in heightening tensions and violence

One of the key aspects of understanding the conflict in Cabo Delgado is the crucial role played by the exploitation of natural resources, particularly natural gas and rubies, in heightening tensions and perpetuating violence.

2.1. Natural Resource Paradox

The Cabo Delgado region, one of the richest in terms of mineral and energy resources, has paradoxically become one of the most impoverished and marginalized in the country. This phenomenon is exemplified by what is commonly referred to as the "natural resource paradox," in which the abundance of resources does not lead to local development but rather to the exacerbation of inequality, exploitation, and violence. The conflict in Cabo Delgado is closely linked to this dynamic, where the exploitation of natural resources not only generates economic and social divisions but also fuels the recruitment of insurgents and the radicalization of young people.

The wealth of natural gas, coal, and rubies in Cabo Delgado has been seen by many as a potential driver of development. However, the reality has been quite different. The

state of poverty and lack of basic infrastructure, such as roads, schools, and hospitals, in a resource-rich province has generated distrust between local communities and the central government. Natural gas exploration, which began with the arrival of large international investors such as the French company TotalEnergies and the American company ExxonMobil, is one of the factors that directly contributed to the intensification of the conflict (Hanlon 2021; Institute for Security Studies 2022).

The impact of natural gas exploration has been negative for many communities in Cabo Delgado, as the benefits of exploration have not reached them. Instead, exploration has been associated with environmental destruction, forced displacement of local populations, and the creation of a highly unequal local economy. The lack of participation of local communities in decisions about how these resources would be explored and distributed has fueled a strong sense of social injustice. This is particularly evident when local communities do not benefit from direct and indirect employment in the gas industries and when foreign companies are perceived as the only ones to profit from this natural wealth, while the population's living conditions remain precarious (Louw-Vaudran 2022).

2.2. Insurgency

In addition, the presence of multinationals and the financing of large projects have generated great competition for resources, with Mozambique's political and economic elites, as well as external forces, having privileged access to these riches. Meanwhile, local youth, who do not have access to the same opportunities, feel increasingly excluded. This economic exclusion has been exploited by insurgents, who have promised an alternative sense of belonging, identity, and reward in exchange for the support of young people and entire families, often through forced recruitment (Hanlon 2021).

The impact of natural resource exploitation on radicalization and recruitment by insurgent groups is one of the most problematic dynamics in Cabo Delgado. The insurgent movement in Cabo Delgado, initially identified as "Al-Shabaab," has presented itself as a local movement that, unlike other jihadist groups, uses arguments of social justice to gain local support. The insurgents exploit the population's resentment towards the exploitation of natural resources, presenting themselves as defenders of the interests of local communities, who feel neglected by the central government and foreign companies operating in the region (Anderson and Olson 2003, 24-86).

The insurgency in Cabo Delgado is not only religious but also sociopolitical in nature. ASWJ (Ahlu Sunnah Wal Jama) is characterized by a rhetoric that aligns with a radical interpretation of Islam, but which largely has a component of resistance to what the insurgents perceive as an unjust political and economic system. The group's leaders use local frustration with poverty and exclusion to recruit young people and build a support base. The provision of financial resources, logistical support,

and a sense of community belonging has been the key to the success of this strategy (Louw-Vaudran 2022).

Furthermore, many young people in Cabo Delgado see themselves as victims of a system that does not provide opportunities. In a region with high unemployment rates and limited educational prospects, the insurgents offer an alternative, offering food, money, and even a promising future, in contrast to the promises of the government and multinationals, which fail to deliver substantial benefits to the local population. This sense of belonging and the promises of financial rewards have been a significant driver of recruitment, which intensifies violence in the region (Institute for Security Studies 2022).

2.3. Government Corruption and Inefficiency

Another key aspect related to the exploitation of natural resources in Cabo Delgado is the negative impact that this exploitation has on local governance and the strengthening of power structures in the province. The lack of central government control over the activities of large multinational corporations and transparency in the licensing and distribution process of resources are issues that directly contribute to the conflict.

Corruption within the central government of Mozambique has been a determining factor in the institutional fragility in the management of natural resources in Cabo Delgado. The licensing process for exploration projects, the allocation of land, and the distribution of benefits generated by the natural gas industry are opaque and are often linked to personal and corporate interests. This results in a system that excludes local communities from any power over their own resources and favors the creation of political and business elites with privileged access to these riches. For many Mozambicans, the government is seen as complicit in the exploitation of natural resources, and this view fuels support for the insurgency, which positions itself against what it considers to be a corrupt and unjust system of governance (Institute for Security Studies 2022; Hanlon 2021).

In addition, the militarization of the region, which occurs as a response to the growing power of the insurgents, is also part of a dynamic of exploitation of natural resources, as local security forces are often more concerned with protecting the investments of foreign companies than with meeting the needs of the local population. In many cases, the military and police have been accused of engaging in human rights abuses, such as looting, killings, and extortion, which contribute to the government's loss of legitimacy and the intensification of conflict (Department for International Development 2002, 12-39).

The exploitation of natural resources without the implementation of inclusive public policies is a critical factor that has fueled violence in Cabo Delgado. The growth of the gas and mining industries in the region has not translated into tangible

benefits for local populations. The central government of Mozambique has failed to implement effective policies to ensure that local communities receive a fair share of the benefits of mineral and energy exploration. The "gas leak", where communities are unable to access the fruits of exploration, has fueled a growing sense of injustice and resistance to government authority. The absence of an inclusive development model, which takes into account the interests and needs of local communities, has been a major cause of instability and violence (Hanlon 2021; Department for International Development 2002, 7-41).

The inequality in the distribution of resources is also evident in the fact that foreign investments in Cabo Delgado have not been channeled towards improving basic infrastructure such as schools, hospitals, and transport systems. Instead, these investments have benefited only a small group of people, while the vast majority of the population continues to live in precarious conditions. Implementing policies that can redistribute resources equitably and promote social inclusion could be an effective measure to destabilize the insurgency, but a lack of political will and corruption in the central government have hindered such actions (Institute for Security Studies 2022).

The exploitation of natural resources in Cabo Delgado is a key factor that has intensified the conflict and exacerbated social and economic tensions in the region. The development model implemented in Mozambique, focused on gas and mineral exploration without a social inclusion strategy, has resulted in inequality, marginalization, and a continuous cycle of violence. The lack of effective public policies, corruption, the exclusion of local communities from the benefits of exploration, and the recruitment of insurgents exploiting this frustration have created an environment of radicalization. For the conflict to be resolved in a lasting way, the Mozambican government and international investors must adopt a more inclusive and transparent development approach, ensuring that the benefits of natural resource exploration reach local communities and promote social peace.

Conclusions

The conflict in Cabo Delgado is one of the most devastating episodes in Mozambique's recent history, and the analysis of this conflict reveals a series of complex dynamics involving both deep and immediate causes, as well as the interaction between local, national, and global factors. The study of underlying causes, such as the historical marginalization of the region, the unequal exploitation of natural resources, and systemic corruption, provides a solid understanding of the reasons why the conflict has persisted and intensified. Throughout this analysis, it was possible to observe how the exploitation of natural resources, in particular natural gas and minerals, plays a central role in the aggravation of social and economic tensions, as well as in the radicalization and recruitment of local youth by insurgent groups.

The role of the exploitation of natural resources as a main cause of the conflict was examined in detail, with a focus on the social and economic impacts of this exploitation. The lack of inclusive public policies, the high degree of inequality, and the absence of a sustainable and equitable development model contributed to the feeling of social injustice in local communities. The exclusion of local populations from the economic benefits generated by resource exploitation, combined with the increasing militarization of the region and corruption within the central government, create a breeding ground for the emergence and perpetuation of the insurgency.

Furthermore, the analysis of the dynamics of recruitment and radicalization by insurgent groups shows how the Cabo Delgado insurgency is not only an ideological struggle but also a response to social, economic, and political issues. The resentment and lack of opportunities faced by local youth, combined with the promise of a better future and the sense of belonging offered by the insurgents, have been powerful drivers of recruitment. This aspect of the insurgency, strongly linked to social and economic issues, represents a major challenge to resolving the conflict, since, in addition to military repression, a real commitment to local development and the fair redistribution of resources is required.

The use of the DFID methodology and other conflict analysis approaches has provided a deeper understanding of the different factors that fuel the conflict and the possible strategies for its resolution. The analysis of the role of natural resources, local governance, the impact of corruption, and the lack of transparency in the exploitation process made it clear that the key to resolving the conflict lies in adopting inclusive public policies, promoting a development model that benefits local communities, and reducing structural inequalities.

In addition, the role of international actors and natural resource companies was also highlighted, showing how the presence of large multinationals can be seen both as an opportunity for development and as a factor in worsening the conflict when their activities are not accompanied by responsible management and a commitment to improving the living conditions of the local population. Transparency in negotiations, the creation of mechanisms to ensure community participation, and the implementation of projects that effectively meet the needs of the population are crucial steps in transforming the exploitation of natural resources into a driver of peace and development, rather than a focus of violence and exploitation.

Therefore, to answer the initial research question, which investigated the impact of natural resource exploitation on the worsening of the conflict in Cabo Delgado, the conclusion is clear: uncontrolled exploitation and the lack of an inclusive development strategy are, in fact, central factors that have fueled violence and insurgency in the region. For the conflict to be resolved effectively and sustainably, it is imperative that the government of Mozambique, in collaboration with investors and the international community, adopt a more just and equitable approach to the management of natural

resources. Only by substantially changing the way resources are managed and distributed will it be possible to reduce the social and economic tensions that fuel the conflict and allow peace and development to come to Cabo Delgado.

Finally, an effective resolution of the conflict requires a sustained commitment to rebuilding Cabo Delgado, including rehabilitating the destroyed infrastructure, implementing social inclusion policies that promote education, health, and employment for local communities, and creating a political and economic environment in which corruption is eradicated and transparency is the norm. This transformation process will require not only strong government action but also the active participation of local communities and the private sector to ensure that Cabo Delgado can overcome its current difficulties and harness its resource potential to promote lasting peace and inclusive development for all its citizens.

References

Anderson, Mary B., and Lara Olson. 2003. *Confronting War: Critical Lessons for Peace Practitioners.* Cambridge, MA: CDA Collaborative Learning Projects. https://www.cdacollaborative.org/publication/confronting-war-critical-lessons-for-peace-practitioners.

Bonate, Liazzat J.K., Paolo Israel, and Cameliza Rosario. 2024. "God, Grievance and Greed: War in Cabo Delgado, Mozambique." *Studia Historiae Ecclesiasticae* (Kronos) 50 (1): 1–23. https://www.scielo.org.za/scielo.php?pid=S0259-01902024000100001&script=sci_arttext.

Department for International Development. 2002. *Conducting Conflict Assessments: Guidance Notes.* Global Social Development Resource Centre. https://gsdrc.org/document-library/conducting-conflict-assessments-guidance-notes/.

Galtung, Johan, and Tord Höivik. 1971. "Structural and Direct Violence: A Note on Operationalization." *Journal of Peace Research* 8 (1): 73-76. https://doi.org/10.1177/002234337100800108.

Hanlon, Joseph. 2017. "Following the Donor-Designed Path to Mozambique's US$2 Billion Secret Debt Deal Catastrophe." *Third World Quarterly* 41 (3): 365–382. doi:https://doi.org/10.1080/01436597.2016.1241140.

___. 2021. "Turning Mozambique into a Mafia, Resource Curse State." *The Round Table: The Commonwealth Journal of International Affairs* 110 (3): 405–406. https://oro.open.ac.uk/78580/.

Independent Commission for Aid Impact (ICAI). 2018. "DFID's Approach to Value for Money in Programme and Portfolio Management. Performance review." https://icai.independent.gov.uk/html-version/dfids-approach-to-value-for-money-in-programme-and-portfolio-management/.

Institute for Security Studies. 2022. "What Drives Violent Extremism in Mozambique?" *ISS Africa.* https://issafrica.org/events/what-drives-violent-extremism-in-mozambique.

International Crisis Group. 2021. *"Mozambique's Insurgency Requires a Multi-Pronged Response."* https://www.crisisgroup.org/africa/southern-africa/mozambique/mozambiques-insurgency-requires-multi-pronged-response.

Louw-Vaudran, Liesl. 2022. "The Many Roots of Mozambique's Deadly Insurgency." *ISS Africa* (Institute for Security Studies). https://issafrica.org/iss-today/the-many-roots-of-mozambiques-deadly-insurgency.

OpenAI ChatGPT. 2024. *Structuring the Paper on the Conflict in Cabo Delgado.* November 19.

Orero, Max Baldwin, Charlotte Heime, Suzanne Jarvis Cutler, and Sarah Mohaupt. 2007. *The Impact of Conflict on the Intergenerational Transmission of Chronic Poverty: An Overview and Annotated Bibliography.* Department for International Development (DFID). https://assets.publishing.service.gov.uk/media/57a08c0eed915d622c0010c7/71Baldwin_Orero_et_al.pdf.

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.
We express our sincere gratitude to Associate Professor Maja Garb of the Faculty of Social Sciences at the University of Ljubljana for her invaluable methodological guidance and academic support throughout the course *Analysis of Contemporary Conflicts*. Her insights and guidance were instrumental in shaping our research.
Last but not least, we are deeply grateful to our families and friends for their support, patience, and encouragement during the preparation of this article.

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 STATEMENT

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

DATA AVAILABILITY STATEMENT

The data supporting this study are derived from publicly available sources and referenced within the article. No additional datasets were generated or analysed specifically for this research.

DECLARATION on AI use

The author confirms that AI tools, including language models such as ChatGPT, 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/

Beijing's Shadow Force: China's Wagner-like Private Security Company in Myanmar's Civil War

Prof. Habib BADAWI*
* Lebanese University, Beirut, Lebanon
e-mail: habib.badawi@ul.edu.lb
ORCID: 0000-0002-6452-8379
SCOPUS ID: 58675152100

Abstract

Purpose: This study examines China's establishment of a joint private security company with Myanmar's military junta as an evolution in Beijing's power projection capabilities. It analyzes how China balances protecting strategic Belt and Road investments while maintaining its non-interventionist diplomatic posture through innovative hybrid security arrangements in conflict zones.

Study design/methodology/approach: The research employs multiple theoretical frameworks to analyze this emerging security paradigm, including securitization theory, graduated sovereignty, and strategic hedging. It synthesizes reports from Myanmar's military-controlled media with comparative analyses of private security companies across different geopolitical contexts, particularly focusing on October 2022-2024 developments in the China-Myanmar Economic Corridor.

Findings: The study reveals China's development of a sophisticated "Wagner with Chinese characteristics" model that differs significantly from Russia's approach to private military contracting. Unlike the Wagner Group's overt combat orientation, China's model emphasizes calibrated influence through corporate structures that provide legal distance while preserving operational control. This arrangement allows Beijing to deploy security elements in sovereign conflict zones without formal military commitment, strategically protecting the China-Myanmar Economic Corridor as an alternative to the vulnerable Malacca Strait.

Originality/value: This research identifies an emerging Chinese doctrine for protecting overseas interests that transcends traditional distinctions between private and state security actors. It demonstrates how China is recalibrating its foreign policy toolkit to include "informal forward deployment" capabilities that operate below the threshold of conventional military intervention. The findings provide a framework for understanding similar hybrid security arrangements that may emerge across Belt and Road territories facing persistent instability.

Keywords:
Belt and Road Initiative; China-Myanmar Economic Corridor; Private Security Companies; Wagner Group; Graduated Sovereignty; Strategic Hedging; Securitization.

Article info
Received: 16 July 2025; Revised: 18 August 2025; Accepted: 12 September 2025; Available online: 6 October 2025

Citation: Badawi, H. 2025. "Beijing's Shadow Force: China's Wagner-like Private Security Company in Myanmar's Civil War". *Bulletin of "Carol I" National Defence University*, 14(3): 138-157. https://doi.org/10.53477/2284-9378-25-40

Throughout history, the ability to project power beyond national borders has distinguished rising powers from established empires. China's Belt and Road Initiative (BRI) now transcends its original development framework, functioning as a sophisticated mechanism for strategic entrenchment across volatile regions (Rolland 2019). At the forefront of this evolution stands Beijing's establishment of a joint Chinese-Myanmar private security company amid Myanmar's civil conflict – a development that represents a calculated recalibration of China's power projection capabilities rather than merely an adaptive business response to instability (Arduino 2018).

On October 22, 2024, Myanmar's military junta established a 13-member committee to draft a memorandum of understanding for this joint security venture (Strangio 2024). This administrative action holds profound strategic significance, signaling China's departure from its established non-interference doctrine. The creation of this quasi-militarized security apparatus – tasked with protecting Chinese infrastructure and personnel – introduces what analysts call an "informal forward deployment" into Beijing's strategic toolkit. As Ghiselli (2021) notes, China's overseas security posture is undergoing a significant transformation as economic interests expand beyond traditional diplomatic frameworks.

This study examines how China has developed a distinctive security approach that differs fundamentally from both Western commercial paradigms and Russia's Wagner Group model. We analyze the strategic imperatives driving this evolution, particularly the critical importance of the China-Myanmar Economic Corridor (CMEC) as an alternative to the vulnerable Malacca Strait (Small 2020). Furthermore, we investigate China's complex diplomatic balancing act in Myanmar - maintaining relationships with multiple actors while incrementally increasing security involvement to protect strategic investments.

The research makes several original contributions to the literature on international security, Chinese foreign policy, and private military contractors. First, it identifies and conceptualizes a distinct "China model" of private security operations characterized by sophisticated integration of commercial legitimacy with state direction (Arduino 2018; Ghiselli 2021). Second, it introduces the concept of "informal forward deployment" to describe China's evolving capability to project power in conflict zones without formal military commitments. Third, it develops a theoretical framework for understanding the "securitization of economic corridors" as infrastructure projects transition from purely commercial endeavors to objects of national security concern requiring protection mechanisms (Buzan, Wæver and De Wilde 1998).

Additionally, the study documents China's shift from traditional non-interference toward what might be termed "calibrated intervention" when core strategic interests are threatened. It provides one of the first comprehensive analyses of how China navigates Myanmar's complex security environment while maintaining relationships

with multiple, sometimes opposing, actors (Kuik 2016). The research offers predictive insights into how similar security arrangements may evolve across other volatile regions where Chinese strategic investments face persistent threats and contributes to theoretical discussions about evolving forms of sovereignty in contemporary international relations (Ong 2006; Bach 2016).

This paper is structured as follows: we first outline the theoretical frameworks employed, then examine the emergence of China's military-commercial hybrid model in Myanmar. Subsequently, we analyze the strategic imperatives driving this development, particularly the importance of securing the China-Myanmar Economic Corridor. We then explore China's diplomatic balancing act in Myanmar's complex conflict environment, compare China's approach with Russia's Wagner Group, and assess the broader implications for China's global security posture. We conclude with reflections on the future of China's power projection capabilities and their implications for international relations theory and practice.

1. Theoretical Framework

This study examines China's joint private security company with Myanmar's military junta through multiple theoretical lenses that collectively illuminate the complex interplay between state power, commercial interests, and security operations in contested environments. The primary theoretical foundation is the "securitization of economic corridors," a process in which strategically significant infrastructure projects shift from being purely commercial undertakings to matters of national security (Ghiselli 2021; Arduino 2018). Drawing on Copenhagen School securitization theory, this framework explains how economic assets become security concerns when exposed to non-traditional threats that jeopardize core strategic interests (Buzan, Wæver and De Wilde 1998). In Myanmar, China's Belt and Road investments—particularly the China-Myanmar Economic Corridor—have undergone this securitization, functioning not merely as economic assets but as strategic alternatives to maritime chokepoints such as the Malacca Strait.

The study also employs Ong's (2006) concept of "graduated sovereignty," which refers to differentiated modes of governance enabling states to exert varying degrees of control across territories without formal annexation. This framework helps explain Beijing's approach in Myanmar, where influence is exercised through a hybrid corporate-security entity that maintains legal distance while ensuring operational control. Related work by Jones and Johnson (2014) on borderland sovereignty and Duara (2006) on "sovereignty regimes" in Asia further contextualizes this phenomenon.

Another key lens is the scholarship on private military and security companies (PMSCs) as instruments of state power (Avant 2005; Kinsey 2006). While early studies viewed PMSCs as independent market actors, recent approaches emphasize

their strategic incorporation into state foreign policy. Cusumano's (2021) "state-directed commercialized security" model provides insight into China's distinctive use of PMSCs, which differs from both Western commercial security models and Russia's Wagner Group paradigm. This framework highlights how states exploit the plausible deniability of private actors while retaining strategic direction.

Strategic hedging theory (Goh 2005; Kuik 2016) is used to analyze China's multifaceted engagement with Myanmar's civil conflict. Rather than strictly balancing or bandwagoning, strategic hedging entails cultivating relationships with multiple—sometimes opposing—parties to maintain flexibility and influence irrespective of conflict outcomes. This framework illuminates China's seemingly contradictory policy of supporting the military junta while simultaneously engaging with opposition forces and ethnic armed groups.
Mann's (1984) concept of "infrastructural power," referring to a state's capacity to penetrate civil society and implement decisions, further enriches the analysis. Bach's (2016) notion of "transnational territorialization" underscores how infrastructure projects such as the China-Myanmar Economic Corridor extend Chinese influence beyond its borders, granting strategic value to the protection of these physical assets.

Together, these frameworks portray China's evolving security approach in Myanmar as a systematic recalibration of power projection capabilities rather than a mere business response. The joint security company embodies a deliberate synthesis of commercial legitimacy and state direction—what this study terms "informal forward deployment"—allowing China to secure strategic corridors without formal military involvement. This model diverges significantly from both Western private security paradigms and the Wagner Group, reflecting China's strategic culture and preference for calibrated influence over overt intervention.

The research adopts a qualitative methodology to analyze China's security operations in Myanmar through these multiple theoretical lenses. Data are synthesized from diverse sources to construct a comprehensive understanding of China's emerging model of private security operations. Primary sources include official statements in Myanmar's military-controlled media, particularly the October 22, 2024, announcement of a 13-member committee tasked with drafting a memorandum of understanding for the joint security venture. These communications reveal how the arrangement is framed and legitimized domestically.

A comparative analysis contextualizes China's model by examining similarities and differences with Russia's Wagner Group, drawing on the framework developed by Badawi and Daabul (2024). Document analysis—of policy papers, official communications, and media reports—constitutes a core methodological approach, aligning with Ghiselli's (2021) method of integrating official discourse analysis with operational realities. Triangulation of multiple data points enables the construction of a coherent picture of China's strategic objectives and operational modalities in Myanmar.

The study employs a multi-theoretical framework bridging international relations, security studies, and political geography, as advocated by Buzan, Wæver and De Wilde (1998). Concepts such as graduated sovereignty (Ong 2006), strategic hedging (Kuik 2016), and infrastructural power (Mann 1984) collectively provide a multidimensional toolkit for understanding China's evolving security posture. Recognizing limitations in available data—especially regarding the company's operational parameters—the study employs theoretical inference based on China's established patterns of private security operations in other regions (Arduino 2018; Badawi 2024b). This approach facilitates reasoned extrapolation while acknowledging the uncertainties inherent in studying emerging security arrangements in contested environments.

2. The Emergence of China's Military-Commercial Hybrid

China's Belt and Road Initiative has evolved from its initial characterization as a development framework to function as a sophisticated mechanism for strategic entrenchment across volatile regions (Rolland 2019). At the forefront of this evolution stands Beijing's establishment of a joint Chinese-Myanmar private security company amid Myanmar's intractable civil conflict. This initiative represents a calculated recalibration of China's power projection capabilities rather than merely an adaptive business response to instability (Arduino 2018).

On October 22, 2024, Myanmar's military junta formally established a 13-member committee to draft a memorandum of understanding for this joint security venture. For China, long committed to non-interference in sovereign affairs, this maneuver signals an unmistakable departure from established doctrine. The creation of this quasi-militarized security apparatus introduces what analysts call an "informal forward deployment" into Beijing's strategic toolkit. The implications extend beyond Myanmar's borders: China appears poised to deploy security elements capable of operating with significant tactical autonomy in a sovereign conflict zone without formally committing People's Liberation Army forces.

This development invites comparisons to Russia's Wagner Group while highlighting the distinctive characteristics of China's approach to militarized commercial engagement. Where Wagner operates with theatrical deniability while maintaining close operational ties to the Kremlin, Beijing's security model embraces a more sophisticated synthesis of commercial legitimacy and state direction. As Badawi and Daabul (2024) observe in their analysis of the Wagner Group, Russia's approach to private military contracting emphasizes overt combat capabilities and direct engagement in conflict environments. China's model, by contrast, reflects what Ghiselli (2021) terms "securitization with Chinese characteristics"—a more nuanced approach that calibrates security involvement according to specific strategic imperatives while maintaining stricter operational discipline.

3. Wagner with Chinese Characteristics: The Evolving Model of Private Security

The parallels between China's emerging security apparatus in Myanmar and Russia's Wagner Group deserve careful examination, revealing both similarities in strategic function and divergences in operational approach. Russia's Wagner Group has operated as a barely concealed extension of state power, engaging directly in combat operations across Africa, the Middle East, and most prominently in Ukraine. As Badawi and Daabul (2024) note, Wagner has functioned as Moscow's "diplomatic special forces"—undertaking missions too sensitive for official military involvement while maintaining sufficient distance to provide the Kremlin with plausible deniability.

China's approach to private security reflects its distinctive strategic culture and foreign policy imperatives. Unlike Wagner's overt combat orientation, traditional Chinese private security companies (PSCs) have typically operated within narrower parameters - primarily focused on site security, risk assessment, personnel protection, and logistical support for BRI projects. Arduino (2018) observes that companies such as Frontier Services Group, China Overseas Security Group, and Hua Xin China Security have established substantial international footprints while generally avoiding direct combat engagements. These entities have operated as genuine commercial enterprises, albeit with close connections to Chinese state interests and security apparatus.

The proposed joint venture in Myanmar, however, represents a significant evolution in this model. By establishing a security company in partnership with Myanmar's military junta, Beijing creates a hybrid entity that transcends the traditional limitations of Chinese PSCs. This corporate structure provides critical advantages: it establishes a legal framework for the importation of weapons and security equipment; it circumvents Myanmar's constitutional prohibition on foreign military deployments; and it creates an operational entity capable of protecting Chinese assets while maintaining the fiction of arm's-length engagement.

This arrangement bears hallmarks of what might be termed "Wagner with Chinese characteristics"—a security force that blends commercial legitimacy with state-directed objectives. Unlike Russia's relatively unrestrained approach to foreign military contracting, China's model emphasizes disciplined integration with broader diplomatic and economic strategies. Badawi (2024a) identifies this distinctive approach as characteristic of China's expanding private security operations globally, which maintain tighter alignment with state objectives and stricter operational parameters than their Russian counterparts. Where Wagner has often operated as a blunt instrument of Russian foreign policy, China's security approach in Myanmar reflects Beijing's preference for calibrated influence and strategic patience.

3.1. The Strategic Imperative: Securing the China-Myanmar Economic Corridor

The China-Myanmar Economic Corridor (CMEC) represents far more than a commercial venture; it constitutes a critical artery in China's grand strategic calculus (Zhao and Yang 2012). As a keystone of the broader Belt and Road Initiative, CMEC comprises an integrated network of highways, railways, pipelines, and economic zones connecting China's southwestern Yunnan province to the deep-sea Kyaukpyu Port in Myanmar's Rakhine State. This corridor offers Beijing a coveted strategic prize: direct access to the Indian Ocean that bypasses the vulnerable Malacca Strait—a maritime chokepoint through which approximately 80% of China's energy imports currently transit (Small 2020).

The strategic significance of this corridor cannot be overstated. In any potential conflict scenario involving the United States and its allies, the Malacca Strait would likely become effectively closed to Chinese shipping - a vulnerability that former Chinese President Hu Jintao famously described as the "Malacca Dilemma" (Wirth 2019). The CMEC represents China's most viable land-based solution to this dilemma, offering an alternative route for energy and trade flows that would remain viable even during maritime blockades or conflicts. As Yeh (2016) argues, China's geo-economic investments increasingly reflect geopolitical imperatives, with energy security and strategic access driving infrastructure development across the BRI footprint.

Yet this strategic corridor crosses some of Myanmar's most volatile regions, where decades of ethnic conflict have been marked by a nationwide civil war following the military coup of February 2021. Since opposition forces declared a "People's Defensive War" later that year, Chinese projects have faced mounting threats (Thuzar 2022). In January 2022, a local People's Defense Force attacked the $800 million Tagaung Taung nickel processing plant. More recently, on October 18, 2024, the Chinese consulate in Mandalay sustained damage in a bombing attack—an incident that occurred in broad daylight in Myanmar's second-largest city, dramatically illustrating the junta's inability to secure even high-priority diplomatic assets.

These security challenges have been exacerbated by the junta's deteriorating position in the civil conflict. The military's grip has become increasingly tenuous, with opposition forces demonstrating surprising resilience and battlefield capabilities. This military overextension has manifested in territorial losses across multiple regions, with opposition forces increasingly capable of operating not only in rural areas but also in urban centers where government control was once assumed.

The vulnerabilities facing the CMEC exemplify what Buzan, Wæver and De Wilde (1998) identify as the process of securitization, whereby economic assets become framed as security objectives when faced with persistent threats. China's incremental shift toward more direct security involvement reflects what Ghiselli (2021) terms the "securitization of overseas interests"—the gradual re-categorization of economic

assets as objects requiring protection through security mechanisms rather than purely commercial arrangements. The joint security company represents the culmination of this securitization process, transforming the protection of infrastructure from a commercial concern to a strategic imperative requiring novel security solutions.

3.2. The Calculus of Intervention: When Economic Assets Become Security Liabilities

Beijing's decision to establish a joint security company reflects a fundamental recalculation of the risk-reward equation in Myanmar. China has historically pursued a policy of "strategic hedging" in Myanmar's internal conflicts - maintaining relationships with the military junta, ethnic armed organizations, and opposition groups simultaneously (Kobayashi and King 2022). As Kuik (2016) observes, strategic hedging allows states to preserve influence across multiple potential outcomes while avoiding firm commitment to any single party. In Table 1 are some of these recent actions.

TABLE NO. 1

China's Strategic Hedging Actions in Myanmar (2021-2025)

Action	Target Actor	Strategic Outcome
Supplying military equipment	Military junta	Strengthened the junta's combat capabilities
Diplomatic pressure on ethnic armed organizations	MNDAA and other groups allied with opposition forces	Protected key economic corridor nodes
Establishing a joint security company	Partnership with the military junta	Created a formal security presence to protect investments
House arrest of the MNDAA commander in Kunming	Pressure on the ethnic armed organization	Attempted to secure withdrawal from strategic Lashio hub
Maintaining communication channels with NUG	Opposition government	Preserved diplomatic flexibility

This approach allowed Beijing to preserve its influence regardless of political outcomes while adhering, at least nominally, to its principle of non-interference in sovereign affairs.

The deterioration of Myanmar's security environment, however, has rendered this balanced approach increasingly untenable. With billions of dollars in infrastructure investments at stake and the strategic imperative of securing an alternative to the Malacca Strait, China has gradually shifted toward more direct involvement in Myanmar's security dynamics. This shift has included supplying military equipment to the junta, utilizing diplomatic pressure on ethnic armed organizations allied with opposition forces, and now establishing a formalized security presence through the joint venture company.

China's intervention reflects a broader pattern observable across its Belt and Road footprint—what might be termed the "securitization of economic corridors" (Fukunaga 2020). In Pakistan, where the China-Pakistan Economic Corridor has faced attacks from Baloch separatists and Islamist militants, Beijing has pressed for enhanced security arrangements, including discussions of joint security companies

(Small 2020). In Central Asia, Chinese private security companies have established growing presences in countries like Kazakhstan and Tajikistan, protecting BRI projects against potential threats (Badawi 2024a). This pattern suggests an emerging doctrine: where economic assets face persistent security threats, China will incrementally escalate its security involvement, calibrating its approach to the specific challenges of each environment.

The Myanmar case is particularly significant because it represents a more advanced form of this intervention. The proposed joint security company would not merely protect static assets but would operate in an active conflict zone where battle lines remain fluid and complex. Moreover, it would function in a political context where China maintains relationships with multiple armed actors—creating potential scenarios where Chinese security personnel might need to navigate engagements with forces that Beijing simultaneously engages with diplomatically.

This evolving approach to security provision represents what Avant (2005) identifies as the strategic use of private security actors to achieve state objectives while maintaining plausible deniability. China's joint security venture in Myanmar exemplifies this pattern, providing Beijing with capabilities to protect strategic assets while preserving diplomatic flexibility and avoiding overt military commitment. The arrangement reflects what Ong (2006) describes as "graduated sovereignty"—the selective application of state power through intermediary entities that allow for calibrated influence without formal territorial control.

3.3. The Mechanics of Deniable Intervention: Structure and Operations

The structure of the proposed joint security company reflects China's careful attention to both legal frameworks and diplomatic optics. By establishing a corporate entity under Myanmar law, with partial ownership by Myanmar interests, Beijing creates a legal foundation for activities that would otherwise violate Myanmar's constitutional prohibition on foreign military deployments. This arrangement provides China with what strategic analysts term as "graduated deniability" – sufficient distance to disavow direct control while maintaining effective influence over operations.

According to reports from Myanmar's military-controlled media, the 13-member committee established on October 22 was specifically tasked with evaluating logistical aspects of importing weapons and security equipment while "ensuring the plan does not undermine Myanmar's sovereignty." This carefully crafted language reflects the political sensitivities surrounding the arrangement, both within Myanmar's military establishment and among its citizens, where anti-Chinese sentiment has periodically erupted in response to perceived encroachments on national sovereignty.

The operational parameters of the joint security company remain officially undisclosed, but several aspects can be reasonably inferred from China's existing private security operations and the specific challenges of the Myanmar environment.

Unlike the Wagner Group's direct combat orientation, the joint venture will likely focus primarily on defensive security - protecting infrastructure, safeguarding personnel, securing transport routes, and conducting threat assessments. Arduino (2018) notes that Chinese PSCs typically emphasize these defensive functions rather than offensive combat operations, reflecting Beijing's preference for minimizing direct involvement in local conflicts while still protecting strategic assets.

The company will likely employ a hybrid staffing model, combining Chinese security specialists (primarily in management, training, and specialized roles) with Myanmar personnel (providing local knowledge, language capabilities, and broader manpower). This approach would mirror China's established patterns in other regions while addressing potential sensitivities around the visible presence of armed Chinese personnel in Myanmar. The command structure would presumably feature formal Myanmar leadership with substantial Chinese influence in strategic and operational decisions - a model that preserves appearances while ensuring Beijing's interests remain paramount.

This organizational arrangement exemplifies what Cusumano (2021) identifies as "state-directed commercialized security"—a model where private security entities maintain formal commercial independence while operating in close alignment with state objectives. The joint venture's hybrid structure provides China with what Jones and Johnson (2014) term "graduated sovereignty"—the ability to exercise influence over security operations in foreign territory without formal territorial control or military deployment. This approach reflects Beijing's sophisticated understanding of how commercial structures can serve strategic objectives while minimizing diplomatic costs and maintaining plausible deniability.

4. The Diplomatic Balancing Act: Multiple Players, Competing Interests

China's establishment of a security presence in Myanmar occurs within a complex diplomatic environment where Beijing maintains relationships with multiple actors. While providing increasing support to the military junta, China has simultaneously preserved channels of communication with the National Unity Government (NUG) and maintained longstanding ties with ethnic armed organizations along the China-Myanmar border.

This multifaceted engagement reflects China's pragmatic assessment that Myanmar's conflict defies simple resolution. The military junta, despite receiving arms and diplomatic support from both China and Russia, has failed to consolidate control over significant portions of the country. Meanwhile, opposition forces—including the NUG, affiliated People's Defense Forces, and allied ethnic armed organizations—have demonstrated surprising resilience but lack the capacity to achieve outright victory in the near term. The result is a protracted conflict with no clear resolution on the horizon.

China's actions suggest a strategic preference for the junta's survival, driven less by ideological alignment than by practical considerations. The NUG's democratic orientation and potential Western alignment represent uncertainties for Beijing, while the junta offers a familiar partner with established relationships. However, China's approach remains fundamentally adaptive - preserving sufficient flexibility to recalibrate should the battlefield dynamics shift decisively against the military regime.

This adaptability was demonstrated in late October 2024 when Chinese authorities reportedly placed Peng Daxun, commander of the Myanmar National Democratic Alliance Army (MNDAA), under house arrest in Kunming. This move aimed to pressure the MNDAA to withdraw from Lashio, a strategic hub in northern Shan State that serves as a gateway between China's Yunnan Province and central Myanmar along the CMEC. The MNDAA's capture of Lashio in August 2024 represented a major strategic setback for the junta, compromising a critical node in the economic corridor.

By intervening directly with the MNDAA, China demonstrated its willingness to leverage relationships with ethnic armed organizations to protect its strategic interests - even while simultaneously deepening security cooperation with the junta. This multidimensional approach reflects what Kuik (2016) identifies as strategic hedging - maintaining relationships with multiple actors to preserve influence regardless of conflict outcomes. China's engagement with both the junta and ethnic armed organizations allows Beijing to protect its core interests while maintaining flexibility to adapt to changing political circumstances.

This sophisticated balancing act exemplifies what Goh (2005) describes as the distinctive characteristics of Chinese strategic hedging in Southeast Asia - the maintenance of multiple, sometimes contradictory relationships that collectively advance core interests while avoiding firm commitment to any single actor. China's approach in Myanmar demonstrates a nuanced understanding of how to navigate complex conflict environments while preserving strategic flexibility and protecting critical infrastructure investments. As Bach (2016) observes, this model of engagement represents a form of "transnational territorialization" that extends influence without formal sovereignty - a pattern increasingly characteristic of China's approach to securing its expanding global footprint.

5. The Wagner Comparison: Shared Functions, Distinctive Approaches

The comparison between China's emerging security model and Russia's Wagner Group (see Table 2) illuminates both common strategic objectives and divergent operational approaches. Both represent mechanisms for extending state influence into contested environments while maintaining degrees of deniability. Both operate at the intersection of commercial interests and geopolitical objectives. And both reflect their parent nations' distinct strategic cultures and foreign policy imperatives.

TABLE NO. 2

Comparison between China's Security Model and Russia's Wagner Group

Characteristic	China's Security Model in Myanmar	Russia's Wagner Group
Legal Structure	Joint venture with the host country's military, emphasizing corporate legitimacy	Quasi-independent entity operating with a minimal legal framework
Operational Focus	Primarily defensive (protecting infrastructure, personnel, transport routes)	Combat-oriented (direct military engagement, training local forces)
Relationship to State	Maintaining disciplined alignment with the centralized strategic direction	Semi-autonomous with considerable operational freedom
Staffing Model	Hybrid staffing combining Chinese management with local personnel	Primarily Russian veterans supplemented by local recruits
Command Structure	Formal local leadership with substantial Chinese influence	Direct Russian military oversight with operational autonomy
Economic Integration	Security as an enabler of broader economic strategies	Securing economic concessions as payment for services
Public Profile	Low profile, emphasis on corporate professionalism	Sometimes flamboyant and deliberately visible
Strategic Emphasis	Calibrated influence and strategic patience	Flexible power projection below the conventional military threshold

Wagner's evolution provides valuable insights into China's potential security trajectory. Wagner initially focused on protecting Russian assets in conflict zones before expanding to direct combat roles, training local forces, securing resource extraction, and conducting political influence operations (Badawi and Daabul 2024). This functional expansion occurred as Moscow recognized Wagner's utility as a flexible instrument of power projection that operated below the threshold of conventional military deployment.

China's security model in Myanmar may follow a similar functional evolution while maintaining distinctive operational characteristics. Rather than Wagner's sometimes flamboyant and deliberately visible approach, Chinese security operations will likely maintain lower profiles, operating with greater discipline and tighter integration with broader diplomatic and economic strategies. As Arduino (2018) observes, Chinese PSCs typically emphasize corporate professionalism and operational restraint compared to their Russian counterparts, reflecting Beijing's preference for subtle influence rather than overt power projection.

The staffing models also differ significantly. Wagner has frequently recruited veterans from the Russian military and security services, supplemented by local forces in theaters of operation. Chinese PSCs have traditionally emphasized recruitment of retired PLA personnel, especially those with specialized skills or experience in overseas operations (Ghiselli 2021). The joint venture in Myanmar will likely follow this pattern while incorporating Myanmar personnel to address both practical and political considerations.

Perhaps most significantly, the integration with economic objectives differs between the two models. Wagner has operated as a quasi-independent actor that secures economic concessions as payment for services – effectively functioning as both security provider and economic exploiter (Badawi and Daabul 2024). China's

model positions security as an enabler of broader economic strategies, with PSCs serving primarily to protect investments rather than to extract resources directly. This distinction reflects China's more systematic approach to economic statecraft, where security elements serve broader strategic objectives rather than functioning as independent profit centers.

These differences reflect what Avant (2005) identifies as distinctive national approaches to the integration of private security actors into foreign policy frameworks. Where Russia has employed private military companies as semi-autonomous instruments with considerable operational freedom, China has developed a more tightly controlled model that emphasizes disciplined alignment with centralized strategic direction. This distinction reflects fundamental differences in strategic culture and institutional organization between the two powers, with China's approach characterized by greater emphasis on coordinated policy implementation and strategic patience.

6. Economic Statecraft and Security Integration: China's Evolving Global Strategy

The establishment of a joint security venture in Myanmar reflects broader patterns in China's evolving global strategy, where traditional distinctions between economic statecraft, security provision, and governance are increasingly blurred. This integration of previously distinct domains represents what Wang and French (2014) identify as China's emerging approach to global economic governance - one that emphasizes institutional flexibility, pragmatic adaptation, and strategic coordination across multiple policy instruments.

The Myanmar case exemplifies what Tsui et al. (2017) describe as "China's strategy for a new global financial order," where infrastructure development serves not merely commercial objectives but functions as a mechanism for reshaping regional governance structures. The China-Myanmar Economic Corridor, like similar initiatives across the Belt and Road footprint, represents what these scholars call a "parallel institution-building" approach that creates alternative channels for Chinese influence while bypassing established Western-dominated frameworks. The securitization of these corridors through hybrid public-private arrangements demonstrates Beijing's recognition that economic entrenchment requires corresponding security capabilities—particularly in volatile regions where state capacity proves insufficient.

This evolution occurs against the backdrop of what Natsios (2020) identifies as a fundamental reconfiguration of foreign assistance in an era of great power competition. Traditional development aid increasingly incorporates security dimensions as donor nations recognize that economic investments remain vulnerable without corresponding protection mechanisms. China's approach in Myanmar—blending infrastructure development with innovative security arrangements—

represents a sophisticated synthesis that transcends conventional categories of foreign engagement. As Natsios observes, "contemporary aid programs increasingly reflect strategic priorities rather than purely humanitarian or developmental objectives" (2020), a clear pattern in China's multidimensional engagement with Myanmar's military junta.

The implications of this approach extend beyond immediate regional contexts to shape broader geopolitical competitions. Thornton (2020) notes striking parallels between China's strategy in Myanmar and its emerging approach in regions like the Sahel, where Beijing similarly confronts the challenge of protecting strategic investments amid persistent instability. In both contexts, China has developed what Thornton terms "calibrated intervention capabilities" that allow for security provision without formal military commitment—a model that has significant implications for European security interests as China's footprint expands across traditional European spheres of influence. The joint security company in Myanmar may thus serve as a prototype for similar arrangements in regions where Chinese economic interests face comparable threats, reflecting Beijing's increasingly sophisticated toolkit for operating in volatile environments.

What emerges from this analysis is a picture of China's Belt and Road Initiative as not merely an infrastructure development program but rather a comprehensive strategy for extending influence through integrated economic, security, and governance mechanisms (Badawi and Mimari 2025). The securitization of economic corridors through hybrid arrangements like the joint venture in Myanmar represents a critical innovation in how rising powers project influence in contested environments—one that may increasingly characterize China's global engagement as its strategic interests expand into regions of persistent instability.

7. Beyond Myanmar: Implications for China's Global Security Posture

The establishment of a joint security company in Myanmar represents more than an isolated response to a specific security challenge—it signals an evolution in China's approach to securing its expanding global interests even in Latin America and the Caribbean (Badawi 2024b). As Beijing's economic footprint has grown through the Belt and Road Initiative, the vulnerability of these investments to political instability, insurgency, terrorism, and criminal activity has become increasingly apparent. The Myanmar model, if successful, could provide a template for similar arrangements in other volatile regions where Chinese interests face persistent threats.

Pakistan's China-Pakistan Economic Corridor (CPEC) presents perhaps the most immediate parallel (Hilali 2019). Following attacks targeting Chinese personnel and projects in Balochistan and other regions, Beijing has pressed Islamabad for enhanced security arrangements. Small (2020) notes that despite Pakistan's establishment of a

Special Security Division of approximately 15,000 personnel dedicated to protecting CPEC projects, attacks have continued—most recently in March 2024, when five Chinese engineers were killed in a suicide bombing. The limitations of Pakistan's security guarantees have prompted discussions of joint security arrangements like those being implemented in Myanmar.

In Central Asia, where China has extensive energy and infrastructure investments, private security companies have already established significant presences. Badawi (2024a) documents how companies such as Frontier Services Group have secured contracts to protect Chinese assets in Kazakhstan, Tajikistan, and other regional states. These arrangements have thus far remained primarily commercial in nature, but the Myanmar model suggests potential for more formalized security partnerships in regions where state capacity proves insufficient to address persistent threats.

Africa represents perhaps the most expansive theater for the potential application of China's evolving security model. With investments exceeding $300 billion across the continent, China faces diverse security challenges—from jihadist insurgencies in the Sahel to political instability in mineral-rich Central Africa. Badawi (2024a) observes that Chinese PSCs have already established presences in multiple African states, but these operations have generally maintained lower profiles and more limited scopes than their Russian counterparts. The Myanmar model could presage more robust security arrangements in African contexts where Chinese investments face heightened threats.

This expanding security footprint reflects what Ghiselli (2021) identifies as the "securitization of overseas interests"—the gradual recognition that economic investments require security protection mechanisms that transcend traditional commercial arrangements. China's evolving approach represents a sophisticated recalibration of how rising powers protect global interests, combining commercial mechanisms with state direction to create security capabilities that operate below the threshold of conventional military deployment. As the Belt and Road Initiative continues to expand across volatile regions, this hybrid security model may become increasingly characteristic of China's global footprint, reflecting Beijing's distinctive approach to power projection in the twenty-first century.

8. The Paradox of Presence: Reconfiguring Power in a Contested World

The emergence of China's joint private security venture in Myanmar represents a profound inflection point in how rising powers navigate the complex terrain between economic entrenchment and security imperatives. Through the theoretical lenses of securitization, graduated sovereignty, and strategic hedging, we can discern not merely an isolated response to localized threats but rather the crystallization of a new doctrine in power projection that may reshape how influence is exercised across contested environments globally.

What distinguishes China's approach is its sophisticated synthesis of commercial legitimacy and state direction—a hybrid model that transcends traditional distinctions between private and state security actors. This "China model" of security operations reflects Beijing's strategic preference for calibrated influence over overt intervention, creating what Mann (1984) might recognize as a new form of infrastructural power that penetrates territories without formal occupation. The joint security company in Myanmar embodies this paradox of presence: simultaneously visible and deniable, commercial yet militarized, local in form yet transnational in function.

The securitization of economic corridors along China's Belt and Road Initiative signals a fundamental recalibration in how infrastructure projects function within national security frameworks. No longer merely conduits for commerce, these corridors have become strategic arteries that demand protection through increasingly sophisticated security arrangements. As Buzan, Wæver and De Wilde (1998) observe in their securitization framework, the designation of economic assets as security objectives transforms how states approach their protection, legitimizing extraordinary measures that transcend normal commercial considerations. The Myanmar case suggests that where traditional diplomacy and commercial security prove insufficient, Beijing is prepared to develop bespoke security solutions that preserve appearances while securing core interests.

This evolution carries profound implications for international relations theory and practice. The Westphalian model of clearly delineated sovereignty encounters new challenges when faced with these hybrid security arrangements that operate across traditional boundaries. Similarly, conventional understandings of intervention must be reconsidered when security operations are conducted through corporate entities with variable degrees of state direction. What emerges is a form of "strategic ambiguity" that allows China to maintain its formal commitment to non-interference while incrementally expanding its security footprint (Enayati 2025).

The theoretical frameworks employed in this study illuminate not only China's approach in Myanmar but potentially a broader pattern as Beijing seeks to secure its global investments against an expanding spectrum of threats. Whether in Pakistan's volatile borderlands, Central Asia's post-Soviet spaces, or Africa's resource-rich conflict zones, the Myanmar model may offer a template for securing strategic interests while minimizing diplomatic costs. As Ong (2006) observes in her analysis of graduated sovereignty, these arrangements represent a fundamental reconfiguration of how power operates in contemporary geopolitics—less through formal territorial control than through calibrated influence exercised through corporate, legal, and security architectures.

Yet this approach contains inherent contradictions that may ultimately prove self-limiting. The same strategic ambiguity that provides flexibility also introduces

uncertainty about command structures, accountability mechanisms, and rules of engagement. As China's security presence expands globally, these ambiguities could generate friction with host nations, competing powers, and local populations. Moreover, the alignment with authoritarian regimes like Myanmar's military junta carries reputational costs that may undermine China's broader diplomatic objectives, particularly in regions where such regimes face mounting domestic and international resistance.

What remains clear is that China's Belt and Road Initiative has entered a more complex phase—one where the projection of influence increasingly requires security capabilities that extend beyond traditional diplomatic and economic tools. In navigating this evolution, Beijing walks a precarious line between protecting its strategic investments and maintaining its carefully cultivated image as a non-interventionist power. The joint security company in Myanmar represents not an endpoint but rather a waystation in this ongoing recalibration—a prototype for what may become a more comprehensive approach to securing China's expanding global footprint.

As this study has demonstrated, understanding these developments requires theoretical frameworks that can capture the nuanced interplay between state power, commercial interests, and security operations in contested environments. The paradox of China's presence in Myanmar—simultaneously engaged yet distant, intervening yet non-interventionist—offers a window into how power may be exercised in an increasingly complex geopolitical landscape, where the boundaries between economic entrenchment and security projection have become increasingly indistinct.

Conclusion: The New Frontier of China's Power Projection

China's decision to establish a joint private security company with Myanmar's military junta marks a pivotal moment in its global Belt and Road calculus. Beyond its stated aim of protecting investments, the initiative signals a deeper, more strategic transformation in China's approach to conflict-prone environments. In choosing to operate through a militarized yet deniable apparatus, Beijing is attempting to thread a needle between preserving its image as a non-interventionist power and securing its increasingly vulnerable geo-economic interests.

The China-Myanmar Economic Corridor (CMEC) is more than a commercial route – it is a strategic artery that underpins Beijing's long-term vision of bypassing maritime chokepoints such as the Malacca Strait. Yet the corridor runs through one of Southeast Asia's most volatile conflict zones. The inability of the Myanmar military to guarantee security, compounded by battlefield losses and diminishing territorial control, has forced Beijing to recalibrate its posture. What emerges is a hybrid model of power projection—where private security functions are fused with state objectives, offering both flexibility and plausible deniability.

Strategically, this development exposes two core realities. First, China's global footprint is maturing from one reliant solely on soft power and infrastructure diplomacy to one increasingly dependent on coercive, hard-power-adjacent mechanisms. The blurring of lines between private security and state military interests is not accidental—it reflects a growing realization in Beijing that safeguarding economic corridors will require force projection capabilities that remain below the threshold of formal military engagement. Second, the move places Beijing in a precarious position within Myanmar's domestic dynamics. While the junta remains China's current partner of convenience, its legitimacy continues to erode. Beijing's overt alignment with an internationally condemned regime could backfire, especially if the junta collapses or if China's security forces are perceived as complicit in repression or violence. Meanwhile, the civilian National Unity Government (NUG) has begun to signal willingness to engage constructively with China, suggesting that Beijing's long-term strategic interests might be better served through more flexible diplomacy rather than rigid support for an increasingly embattled regime.

At the operational level, the Myanmar case offers a model for future Chinese interventions in similar theaters—such as Pakistan, Central Asia, or parts of Africa—where BRI assets intersect with fragile states and insurgent threats. However, the risks are mounting. Should Chinese personnel be drawn into confrontations or implicated in rights abuses, the reputational and geopolitical costs could undermine the very strategic interests China seeks to preserve.

In essence, China's move into Myanmar's security space is both reactive and preemptive: a response to current insecurity and a signal of evolving doctrine in overseas power protection. But as it evaluates the limits of indirect militarization, Beijing must also contend with a paradox—protecting its empire of infrastructure may ultimately require choices that undermine the very principles of sovereignty and non-interference it has long championed.

Whether this experiment in security outsourcing stabilizes China's position in Myanmar—or entangles it further in the quagmire of civil conflict—remains to be seen. What is certain, however, is that China's Belt and Road Initiative has entered a new and more dangerous phase, one where concrete and steel are no longer sufficient safeguards without the shadow of the gun.

References

Arduino, A. 2018. *China's private army: Protecting the New Silk Road*. Palgrave Macmillan.

Avant, D. 2005. *The force market: The consequences of privatizing security*. Cambridge University Press.

Bach, D.C. 2016. *Regionalism in Africa: Genealogies, institutions, and trans-state networks*. Routledge.

Badawi, H. 2024a. "China's stealthy expansion: Dark horizons of global private security contractors." *Journal of Afro-Asian Studies* 20: 39–72. Democratic Arabic Center. https://democraticac.de/?p=94611

___. 2024b. "The Dragon's overwatch: Chinese private security expansion in Latin America and the Caribbean." *Bulletin of "Carol I" National Defense University* 13(3): 7–26. https://doi.org/10.53477/2284-9378-24-27

Badawi, H., and M. Daabul. 2024. "The Wagner Group: Complex web of intrigue and geopolitics structure." *Arab Journal for Security Studies*, 40(2): 262–282. https://doi.org/10.26735/PLCX8094

Badawi, H., and A. Mimari. 2025. *The Belt and Road Initiative: The revived strategy for China's supremacy* (pp. 18–58). Democratic Arabic Center. https://democraticac.de/?p=102368

Buzan, B., O. Wæver, and J. De Wilde. 1998. *Security: A new framework for analysis*. Lynne Rienner Publishers.

Cusumano, E. 2021. *Guns for hire: The international market for private military and security services*. Oxford University Press.

Duara, P. 2006. "The new imperialism and the post-colonial developmental state: Manchukuo in comparative perspective." *The Asia-Pacific Journal* 4(1): 1–18.

Enayati, A. 2025. "Deciphering China's military space program and its global strategic components." *Strategic Defense Press*. https://www.researchgate.net/publication/389299554_Deciphering_China%27s_Military_Space_Program_and_Its_Global_Strategic_Components

Fukunaga, Y. 2020. *ASEAN's institutional and legal framework for managing relations with external partners*. In S. H. Ali (Ed.), *Asia's regional architecture: Alliances and institutions in the Pacific century* (pp. 295–314). Edward Elgar Publishing. https://www.elgaronline.com/monochap/9781788977463.00019.xml

Ghiselli, A. 2021. *Protecting China's interests overseas: Securitization and foreign policy*. Oxford University Press.

Goh, E. 2005. *Meeting the China challenge: The U.S. in Southeast Asian regional security strategies*. East-West Center Washington.

Hilali, A.Z. 2019. "China-Pakistan Economic Corridor and dynamics of regional connectivity: Prospects and challenges." *Strategic Studies* 39(4): 89–103. https://www.jstor.org/stable/48732323

Jones, L., and C. Johnson. 2014. *Placing the border in everyday life*. Routledge.

Kinsey, C. 2006. *Corporate soldiers and international security: The rise of private military companies*. Routledge.

Kobayashi, Y., and J. King. 2022. "Myanmar's strategy in the China–Myanmar Economic Corridor: A failure in hedging?" *International Affairs* 98(3): 1013–1032. https://doi.org/10.1093/ia/iiac049

Kuik, C.C. 2016. "How do weaker states hedge? Unpacking ASEAN states' alignment behavior towards China." *Journal of Contemporary China* 25(100): 500–514.

Mann, M. 1984. The autonomous power of the state: Its origins, mechanisms, and results. *European Journal of Sociology* 25(2): 185–213.

Natsios, A.S. 2020. Foreign aid in an era of great power competition. *PRISM* 8(4): 100–119.

Ong, A. 2006. *Neoliberalism as exception: Mutations in citizenship and sovereignty*. Duke University Press.

Rolland, N. 2019. A China–Russia condominium over Eurasia. *Survival* 61(1): 7–22. https://doi.org/10.1080/00396338.2019.1568043

Small, A. 2020. "The China-Pakistan Economic Corridor: Strategic rationales, external perspectives, and challenges to effective implementation." *Asia Policy* 27(4): 27–43.

Strangio, S. 2024. "China, Myanmar to establish joint security company, reports say." *The Diplomat*. https://thediplomat.com/2024/11/china-myanmar-to-establish-joint-security-company-reports-say/

Thornton, P. 2020. "Beijing's 'going out' strategy and Belt and Road Initiative in the Sahel: Security implications for European interests." *The International Spectator* 55(4): 15–29.

Thuzar, M. 2022. The Myanmar crisis and ASEAN: Implications, opportunities and limitations (Chapter 4). In *NIDS Joint Research Series No. 20*. National Institute for Defense Studies. https://www.nids.mod.go.jp/english/publication/joint_research/series20/pdf/chapter04.pdf

Tsui, S., E. Wong, L. Chi and W. Tiejun. 2017. One Belt, One Road: China's strategy for a new global financial order. *Monthly Review* 68(8): 36–45.

Wang, H., and E. French. 2014. "China in global economic governance." *Asian Economic Policy Review* 9(2): 254–271.

Wirth, C. 2019. Broadening horizons: "Indo-Pacific" maritime politics beyond China (*GIGA Focus Asia*, No. 6). *German Institute for Global and Area Studies (GIGA)*. https://www.giga-hamburg.de/en/publications/giga-focus/broadening-horizons-indo-pacific-maritime-politics-beyond-china

Yeh, E.T. 2016. Introduction: The geoeconomics and geopolitics of Chinese development and investment in Asia. *Eurasian Geography and Economics* 57(3): 275–285.

Zhao, H., and M. Yang. 2012. China-Myanmar economic corridor and its implications. *East Asian Policy* 4(4): 64–75. https://doi.org/10.1142/S1793930512000128

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Risk of Military Expansion in the Democratic Republic of Congo: A Threat of Wider Regional Conflict

Christopher ODHIAMBO*

*Masters of Science in Governance, Peace, and Security Studies, Africa Nazarene University
e-mail: codhiambo878@gmail.com
https://orcid.org/0009-0007-4975-788X

Abstract

As military clashes between the M23 rebel group, purportedly supported by Rwanda and Uganda, intensify, the Democratic Republic of the Congo (DRC) is once again at risk of regional instability. This paper looks at the dangers of military growth in the Democratic Republic of the Congo and how it might lead to a wider Great Lakes conflict. The research focuses on the roles of important players, such as MONUSCO, regional alliances, and international actors assisting insurgent organizations, and draws on current geopolitical developments. It contends that there are serious risks to regional peace and security from the further militarization of the conflict if its underlying political and socioeconomic roots are not addressed. The study highlights the necessity of political commitment to lasting peacebuilding and revitalized diplomatic structures.

Keywords:

Democratic Republic of Congo (DRC); M23; MONUSCO; Regional Conflict; Great Lakes Region; Peacekeeping; Military Expansion.

Article info

Received: 10 July 2025; Revised: 7 August 2025; Accepted: 1 September 2025; Available online: 6 October 2025

Citation: Odhiambo, C. 2025. "The Risk of Military Expansion in the Democratic Republic of Congo: A Threat of Wider Regional Conflict" *Bulletin of "Carol I" National Defence University*, 14(3): 158-165. https://doi.org/10.53477/2284-9378-25-41

Introduction

African interlocutors and external actors need to act quickly to prevent the bloodshed in the Great Lakes Region, since the possible factors in a shifting political calculation could be behind the sponsors of the March 23 Movement (M23) rebel group beginning another conflict. DRC is also a place that is yet to recover after the disastrous Congo Wars of the late 1990s and early 2000s, when the militaries of seven African States intervened and took part in the Congo, killing up to an estimated 5.4 million Congolese people (Fabricius 2024a).

In the Democratic Republic of the Congo (DRC), besides the 6,000 estimated M23 soldiers, there are about 4,000 Rwandan soldiers, and there is also evidence from UN investigators that M23 has Ugandan backing (Africa Centre for Strategic Studies 2022). The troops of M23 rebels have already taken over the city of Goma, and this has created shockwaves throughout the region, and a bigger war in this region is imminent (International Crisis Group 2025). It is particularly worrying that this development comes at a time when it is highly considered that M23 is backed by the Rwanda Defense Force (RDF), as Rwanda still has interests in the DRC.

Problem Statement

The United Nations has been active in the region, as well as in the Democratic Republic of Congo, since the start of 1999. At first, the organization was present in the country with its peacekeeping forces, under the United Nations Organization Mission in the Democratic Republic of the Congo (MONUC) mandate. In 2010, the mission was changed to the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO).

Nowadays, the UN Mission has the strength of over 1500 members, including combat soldiers, a peacekeeping army charged with the responsibilities of conducting focused war attacks in an effort to eliminate groups perceived to be a menace to the state power (Nantulya 2024). Security in the DRC is also not in a good state, with the primary aggressors being rebel groups and criminal organizations. Nevertheless, the armed community-based self-defense groups are on the increase. MONUSCO has been reacting to this trend through aerial activities and undertaking short-term measures that focus on the enhancement of the defense of civilians, which is by integrating well-trained police-military patrols in its plans. The organization has also engaged more soldiers to deal with the high tensions that have hounded the communities (Africa Centre for Strategic Studies 2022). Although this has been done, it seems that there is no commitment to neutralizing the conflict. This has, however, been lacking in operational coordination between MONUSCO and other forces due to the reports of violent operations among other forces.

This paper argues that the ongoing military expansion in the eastern Democratic Republic of Congo, driven by the resurgence of the M23 rebel group and the involvement of regional actors like Rwanda and Uganda, poses a significant threat to regional stability and peace, and that without a shift from militarized responses to comprehensive political and diplomatic engagement, the Great Lakes Region risks relapsing into widespread conflict.

Background

The conflict in DRC, which has been ongoing for more than two decades, has had negative implications for the country's socio-economic and political outcomes despite the presence of international actors such as the United Nations. The UN's unsuccessful peacekeeping operation in the Democratic Republic of the Congo should be stopped slowly and receptively. The need to avoid a security gap within the country created by the DRC war is overstressed. The spread of the 23 March Movement (M23) across the country, including such places as North Kivu, has raised deep concern, in particular, for the secretary of the United Nations Organization Stabilization Mission in the Democratic Republic of the Congo (MONUSCO) (Fabricius 2024a). Actually, considering the fact that the analysts believe Rwanda has increased its support to M23, this rapid escalation can, in all probability, trigger a broader regional conflict.

MONUSCO has already trained many recruits of the DRC government, called the Armed Forces of the Democratic Republic of Congo (FARDC), who are set to protect Sake and Goma against the M23. Since the Southern African Development Community (SADC) has been authorized by the African Union to deploy forces at the regional level, the regional force is yet to achieve full operating capacity (International Crisis Group 2025). In case the conflict in the region continues, the countries surrounding the area also face a risk of spill-over in the Greater Lakes region, and this is likely to lead to an even more devastating impact, as indicated in a report submitted by Sierra Leone, Algerian, Mozambican, and Guyana representatives (Nantulya 2024). Moreover, Japanese representatives claimed that enhanced military activities by the gangs, like M23, ruined the lives of communities besides posing a threat to human security. In that sense, the support given to M23 and other armed militia should be halted since the further display of such support can end up jeopardizing the region to the brink of massive war (Africa Centre for Strategic Studies 2022).

In another report, prepared by the Russian Federation, it was indicated that, although it is commonly referred to as a forgotten crisis, it is one of the oldest and bloodiest conflicts with no match in casualties so far (Fabricius 2024b). It happens to be quite unfortunate that efforts that have been made on the diplomatic front have amounted to limited achievements, thus the need to have countries that have economic and political interests influence the parties that matter.

The United States was also an advocate of the fact that operations of MONUSCO in North Kivu must continue until more improvement is made (International Crisis Group 2025). This was why, in their opinion, Rwanda, as a major troop-contributing nation in UN peacekeeping operations, could not tolerate the conduct of the M23 members. Consequently, there has to be a solution to allow the Congolese to stabilize their eastern province and Rwanda to maintain internal security.

The international peacekeeping force created in the Democratic Republic of Congo has existed long enough, and such an operation ought to be slow and cautious. It is strongly stressed that the conflict in the DRC needs to be counteracted to avoid a vacuum in domestic security. The secretary of MONUSCO has expressed concerns over the recent explosive rise of the M23 across the country, particularly in regions of the country such as North Kivu (Nantulya 2024). Also, given that analysts believe that Rwanda has stepped up its support to M23, this sudden development is fraught with the strong likelihood of prompting an even greater regional war.

Justification of the Study

The fragile balance of peace in the Great Lakes Region, which encompasses nine neighbouring states, is also under jeopardy because of the ongoing instability in the eastern Democratic Republic of the Congo. Concerns reminiscent of the First and Second Congo Wars are raised by the reappearance of violence involving numerous state and non-state entities. The M23's comeback and the participation of surrounding nations point to a structural breakdown in the current conflict resolution processes, notwithstanding years of peacekeeping missions and regional diplomacy. The pressing need to evaluate the effects of military expansion in the DRC, investigate the possibility of regional spill-over, and pinpoint avenues for a long-term political resolution justifies this study. The research also contributes to the literature on African conflict dynamics, peacekeeping missions' effectiveness, and international mediation efforts.

Methodology

The qualitative research design used in this study is based on desk-based content analysis. It synthesizes information from scholarly publications, regional policy declarations, official UN reports, and journalistic inquiries from reliable sources, including the Institute for Security Studies, the Africa Center for Strategic Studies, and the International Crisis Group. The approach enables a critical analysis of the conflict's military, political, and diplomatic aspects. The study uses a theme approach to evaluate the efficacy of diplomatic and peacekeeping efforts, player motivations, and regional ramifications. Triangulation of data is used to improve the reliability and validity of results.

Expansion of Conflict outside Congo

Goma, the capital of the strategically important and mineral-rich North Kivu Province in the eastern Democratic Republic of the Congo (DRC), was well-planned and accomplished. This capture continues M23's expanding push to regain control of territory in the eastern DRC, which began in 2022 (International Crisis Group 2025). Alongside this, there have been initiatives to boost resource exploitation and create a parallel civilian administration in regions under M23 control. This implies that maintaining and maybe extending their geographical control is a longer-term goal for the rebel organization and their local supporters.

At least 17 peacekeepers, including those from the Southern African Development Community (SADC) serving in MONUSCO, have been killed; hospitals are overrun with casualties, many of whom are civilians; businesses and shops are being looted; heavy ordnance is landing in civilian areas; and the attacks have caused a major humanitarian crisis, forcing displaced people to flee further south in the already unstable South Kivu or across the Rwanda border (International Crisis Group 2025). Since January 2024, over 500,000 people have been displaced. Hundreds of angry demonstrators in Kinshasa are calling on the government to act swiftly and forcefully to retake the lost land (Fabricius 2024a). Others are demanding firearms so they can join the battle in the east, while others have set fires in front of Western embassies in protest of the international community's inability to put an end to the violence.

There is intense pressure on Congolese President Félix Tshisekedi to address the violence, which is generally assumed to be originating from Rwanda and Uganda (Fabricius 2024a). With Kisangani, Bunia, Bukavu, and Goma serving as key epicentres, the Congo wars of the 1990s and 2000s also began in eastern DRC, and eventually, seven African militaries were involved. The regional anxiety is fuelled by fears that Rwanda, which has about 10 percent of the DRC's population, would gain disproportionate influence over one of Africa's largest countries with nine neighbours (International Crisis Group 2025). The regionalization of the conflict further complicates efforts to find solutions to fundamental political and social issues.

In 2012, M23 strategically managed to take over the city of Goma, which is considered a strategic location in the country. Today, the group is even larger and more organized and armed and comprises well-trained personnel, making it a force that necessitates special attention. Since 2022, M23 has managed to carry out multiple strikes and attacks, resulting in the capture of large areas such as the provinces in the North and South Kivu (Nantulya 2024). The use of its heavy artillery, combat drone, and surface-to-air missiles confirms the argument that they enjoyed massive state support. Also, their equipment and uniforms show that they do not look like a mixed crew.

As a former guerrilla fighter and retired South African Army General, Maomela Motau shared his account of the nature of and tactics used by the guerrilla fighters to understand what is going on in DRC. His account reveals that M23 fighters must be supported by a strong force or group. Another complex issue is the dynamic regionalist relationships of Burundi, Rwanda, Uganda, and the Democratic Republic of the Congo (International Crisis Group 2025). Burundi and DRC have as many as 10,000 troops with an Imbonerakure government militia in the eastern region (International Crisis Group 2025). People on the ground fear that any time the violence might break out, since more Congolese troops are leaving Goma in boats to the town of Bukavu in South Kivu, where Burundian forces are based.

It is also crucial to note that the Goma assault occurred in a different security environment. During the early periods of the war, Uganda used to fight alongside Rwanda. This implied that despite Uganda being bitter enemies with Rwanda today, it was not at the time antagonistic to M23 when it seized control of Goma in 2012. Some 1,000 members of the M23 disappeared in 2014 (a group of fighters was disarmed and cantoned in Rwanda) after the group was disbanded in 2013 and cantoned in a military base in western Uganda (International Crisis Group 2025). After concluding a deal with the DRC, Uganda is now building new roads, bridges, and other infrastructure in North Kivu in 2021, starting with the road between Bunagana and Rutshuru, Goma, and all the way to the Rwandese border. Rwanda and Uganda have been marred with military activity in the Democratic Republic of the Congo since the two countries had initially joined forces and successfully battled with a single military force against the Congolese longstanding ruler, Mobutu Sese Seko, during the First Congo War. Later, they engaged in battle on the Congolese territory during the Second Congo War in favor of opposing factions that were interested in overthrowing the government of Laurent Kabila. It is therefore difficult to know how the top military leaders of the two countries will behave in the latest escalation of hostilities, judging by the previous rush of activities between them.

Recommendations

There are so many uncertainties in the rapidly developing crisis in the eastern Democratic Republic of the Congo. One thing remains the same, though. The background political, social, and economic issues that have given rise to instability are not issues that can be helped by a military reaction. Already, there exists a mechanism to handle the outer facets of the crisis of the neighbours and the internal conflict of the DRC, like the nationality and citizenship problems. The Sun City Accords that were signed as the culmination of the Inter-Congolese Dialogue (ICD) in 2001 through 2003 created a model of a comprehensive peace that addressed deep-rooted leadership of both political and socioeconomic problems in Congo. The external features of the issue were managed through the simultaneous Lusaka Peace Accord. The result of both processes and the localization of the framework in the unstable Ituri region was the establishment of the International Conference on

the Great Lakes Region (ICGLR), a UN engagement tool, which helps to commit all parties. In a bid to lure Rwanda and the DRC into political interaction, two lines of operation, i.e., the Luanda process, led by Angolan President Joao Lourenco, and the Nairobi process, led by Kenyan President William Ruto, would reawaken some of this institutional recall and expertise. To renew the structures of dealing with the root causes and give new life to these discussions, the immediate issue is to create the political desire to de-escalate.

Conclusion

The violence in the eastern Democratic Republic of the Congo is a tense intersection of regional rivalries, unresolved socio-political issues, and old grievances rather than a singular internal problem. The M23 rebel group's comeback, which has reportedly received support from Rwanda and Uganda, highlights how consistently national and international actors have failed to put long-term peace frameworks into action. Even though MONUSCO and other peacekeeping missions have brought about some temporary security, their effectiveness has been hampered by a lack of political will, coordination, and sincere dedication to resolving the conflict's underlying issues.

A wider regional conflict similar to the catastrophic Congo Wars of the past could be rekindled by the crises' increasing militarization, especially the deliberate takeover of areas like Goma. Thus, the Great Lakes Region continues to face a significant danger of conflict escalation in the absence of a firm shift toward inclusive discourse, regional diplomacy, and long-term development plans. In addition to the removal of foreign interference, legal Congolese institutions must be empowered, and regional peace mechanisms like the Luanda and Nairobi processes must be reactivated, for the DRC to experience sustainable peace. Reactive initiatives have outlived their usefulness; instead, principled, coordinated, and proactive diplomacy must be prioritized.

References

Africa Center for Strategic Studies. 2022. "Rwanda and the DRC at Risk of War as New M23 Rebellion Emerges: An Explainer." https://africacenter.org/spotlight/rwanda-drc-risk-of-war-new-m23-rebellion-emerges-explainer/.

Fabricius, Peter. 2024a. *Military muscle rather than mediation prevails in DRC*. Institute for Security Studies. https://issafrica.org/iss-today/military-muscle-rather-than-mediation-prevails-in-drc.

___. 2024b. *Once more into the breach: SADC troops in DRC.* Institute for Security Studies. https://issafrica.org/iss-today/once-more-into-the-breach-sadc-troops-in-drc.

International Crisis Group. 2025. "Fall of DRC's Goma: Urgent Action Needed to Avert a Regional War." https://www.crisisgroup.org/africa/great-lakes/democratic-republic-congo/fall-drcs-goma-urgent-action-needed-avert-regional-war.

Nantulya, Paul. 2024. *Understanding the Democratic Republic of the Congo's Push for MONUSCO's Departure.* Spotlight. Africa Center for Strategic Studies.

ACKNOWLEDGEMENTS
We also acknowledge the authors and institutions whose online publications, reports, and databases provided the basis for this study.

FUNDING INFORMATION
This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

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
This research is based on secondary data and publicly available online resources. All sources consulted are appropriately cited within the manuscript. Additional data supporting this study may be accessed through the references provided.

DECLARATION on AI use
The authors maintained full responsibility for the intellectual content, interpretation of data, and conclusions.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

From Norms to Practices: Equal Treatment and Territorial Justice in the Hungarian Military

Dr. Makkos NÁNDOR, PhD*

*National University of Public Service, Hungary
e-mail: nandor.makkos@tef.gov.hu
https://orcid.org/0000-0001-8978-3870

Abstract

This study probes the disconnect between formal equality mandates and day-to-day realities in the Hungarian Defence Forces, framed by NATO/EU commitments and Hungary's own legal framework. Using a mixed-methods design – including policy analysis, interviews, focus groups, and observations – the authors blend enlistment statistics (15,482 U.S. records; 2,481 Hungarian surveys modelled via Bayesian hierarchies) with personal narratives that expose how economic pressures, gender norms, and regional stigma drive recruitment. Results uncover clear urban–rural divides in compliance, reveal that grievance procedures are undermined by mistrust, and identify unit-level leadership as the linchpin for meaningful equality. This study examines how the Hungarian Defence Forces' formal equality mandates – grounded in NATO, EU, and national law – are undermined by economic pressures, gender norms, and spatial disparities, revealing that only committed unit-level leadership and tactical initiatives like Gender Focal Points, hybrid deployments, and the "Forward Together" mentoring programme can bridge the gap between paper compliance and genuine cultural transformation.

Keywords:
Equal Treatment; Spatial Justice; Hungarian Defence Forces; Bayesian Hierarchical Modelling; Intersectional Mentoring.

Article info
Received: 7 July 2025; Revised: 1 August 2025; Accepted: 1 September 2025; Available online: 6 October 2025

Citation: Nándor, M. 2025. "From Norms to Practices: Equal Treatment and Territorial Justice in the Hungarian Military". *Bulletin of "Carol I" National Defence University*, 14(3): 166-184. https://doi.org/10.53477/2284-9378-25-42

1. Introduction and Research Questions

Over the past two decades, the global defence sector has undergone a paradigmatic transformation. The expansion of the security concept, which now includes not only external threats but also internal legitimacy, social justice, and human rights, has redefined the operational environment of modern armed forces. In this evolving landscape, ensuring equal treatment and promoting equal opportunity are not solely legal or ethical obligations. They have become key components of operational effectiveness, impacting cohesion, strategic credibility, and overall mission success.

For NATO member states such as Hungary, the normative foundations of inclusion, dignity, and non-discrimination are reflected in both international expectations and domestic legal frameworks. The Hungarian Defence Forces (HDF) are formally bound by these commitments through their integration into Euro-Atlantic structures. However, the practical implementation of these norms remains deeply influenced by local institutional cultures, leadership dynamics, and socio-political conditions.

Hungary presents a particularly revealing case. While national legislation, including the Fundamental Law and the Equal Treatment Act (ETA), endorses equality principles, and while NATO's 2022 Strategic Concept emphasises inclusive security and democratic resilience, implementation outcomes continue to vary. Empirical studies point to persistent disparities across military units and geographic regions, revealing a territorial gradient of inclusion that mirrors broader social inequalities (Demeter 2022; Clomax, et al. 2024).

This article contends that organisational culture alone cannot fully account for this variation. Building on Edward W. Soja's concept of spatial justice, Robert Sack's theory of human territoriality, and Doreen Massey's idea of power geometry, we interpret the "military corridor" as a territorially embedded state strategy. This mechanism redistributes the social costs and risks of national defence by concentrating recruitment efforts in marginalised areas. In the United States, this corridor extends through the rural Deep South, while in Hungary, it is anchored in the deindustrialised eastern regions. These areas – characterised by structural poverty, limited civilian opportunities, and social stigma – have become focal points for recruitment, especially among women and ethnic minorities.

Although Hungarian defence policy documents express formal alignment with NATO values, a significant implementation gap remains. This study addresses that gap by applying a combined institutional and spatial lens, supported by qualitative methods including policy analysis, semi-structured interviews, and organisational mapping. The analysis is further strengthened by a cross-national comparative dataset comprising 17,963 quantitative enlistment records and 120 qualitative focus group narratives.

Research Questions

To what extent have equality and non-discrimination principles been effectively operationalised and internalised within the Hungarian Defence Forces?

What organisational and spatial factors facilitate or hinder the realisation of substantive equality?

How do NATO norms and external legal obligations influence internal military governance and equal treatment practices in Hungary?

Objectives

This study aims to:

- Map the relevant international and domestic normative frameworks;
- Evaluate the practical implementation of these norms using empirical data;
- Offer policy recommendations to improve human resource practices in the defence sector.

Article Structure

Section 2 presents the theoretical framework, drawing on Soja, Sack, Harvey, and Massey to develop a lens of territorial equity. Section 3 maps recruitment disparities in Hungary and the United States using Bayesian hierarchical modelling. Section 4 analyses focus group data to explore lived experiences within military recruitment corridors. Section 5 synthesises findings into four actionable policy levers. Section 6 outlines the data and methods used, ensuring reproducibility. Section 7 concludes by arguing that national security is inseparable from spatial justice and that without geographical awareness, inclusion remains symbolic rather than substantive.

2. Theoretical Framework and Normative Context

This study draws upon interdisciplinary insights from new institutionalism, legal sociology, and critical compliance scholarship to examine how formal norms of equality and non-discrimination are embedded, interpreted, and contested within military organisations. At the heart of this theoretical framework lies the proposition that legal norms are not simply adopted or rejected; rather, they undergo complex processes of "translation" as they move from abstract commitments to concrete institutional practices.

Vivien Lowndes and Mark Roberts (2013) describe norm translation as the selective adaptation of external legal or policy expectations into locally intelligible practices, often shaped by institutional path dependencies, cultural codes, and routines. In the case of military organisations – especially hierarchical ones like the Hungarian Defence Forces (HDF) – these mediating factors are particularly influential. The values of command, discipline, and unit cohesion often take precedence over deliberation, inclusion, or participatory governance, which may lead to the dilution or instrumentalisation of equality norms.

In Hungary, the dual pressures of EU membership and NATO integration have created a dense web of legal and political commitments aimed at ensuring equal treatment within the armed forces. Domestically, Article XV of the Fundamental Law of Hungary guarantees equality before the law and the prohibition of discrimination. This is further elaborated by Act CXXV of 2003 on Equal Treatment and the Promotion of Equal Opportunities, which provides legal protection against discrimination on grounds such as gender, ethnicity, religious affiliation, and political opinion. The Act mandates both preventive and remedial measures and applies to public sector institutions, including the military.

Internationally, Hungary is bound by NATO's 2022 Strategic Concept, which articulates gender equity, democratic accountability, and social inclusion as essential components of allied resilience. This commitment aligns with the European Union's Directive 2000/78/EC, which prohibits discrimination in employment and occupation. It also reflects the growing consensus within international humanitarian law (IHL) and human rights regimes that adverse distinctions in access to public service, including military careers, must be justified only under the most stringent conditions.

However, compliance with these frameworks is not merely a technical matter of aligning statutes. Rather, it is a deeply political and symbolic process. The diffusion and internalisation of norms depend on several factors: high-level leadership commitment, organisational capacity to enforce regulations, and the legitimacy of these norms in the eyes of personnel. As a result, equal treatment is not only a legal-institutional concept but also a site of ongoing negotiation – among commanders, policy-makers, and soldiers – about the values and identities that the armed forces are expected to embody.

The literature on military sociology has long debated whether cohesion and diversity are compatible. Earlier theories, such as those of Moskos (1968), viewed social representation as a potential threat to combat effectiveness, arguing for a cautious approach to inclusion. However, more recent work (King 2013; Carreiras 2006) demonstrates that diverse units can perform exceptionally well when supported by inclusive leadership and coherent policy frameworks. Diversity, far from undermining unity, can enhance adaptability, innovation, and legitimacy – especially in international missions where trust with local populations is crucial.

In parallel, gender mainstreaming has become institutionalised through mechanisms such as NATO's Bi-Strategic Command Directive 40-1. Yet, critics warn that mainstreaming often remains procedural, focusing on metrics and checklists without addressing deeper cultural resistances (True 2016). Intersectionality, as introduced by Crenshaw and extended in military scholarship (Ni Aoláin, Haynes and Cahn 2011), compels us to look beyond "gender" as a homogeneous category and consider how race, class, and sexual orientation co-construct the lived experience of inclusion or exclusion.

Post-socialist militaries like the HDF face additional constraints stemming from transitional legacies: politicised promotion systems, fragmented civilian oversight, and a lingering distrust of external monitoring mechanisms. These institutional conditions render the implementation of equality norms particularly complex and, at times, contradictory. Scholars such as Szvircsev-Tresch (2014) and Makkos (2024) note that formal legal alignment often masks informal organisational cultures that resist change or reproduce hierarchical exclusions.

Against this backdrop, the theoretical framework adopted in this study serves two purposes. First, it offers a lens to analyse the gap between normative ambition and institutional reality – what has been termed the "policy–practice gap." Second, it enables a grounded exploration of how spatial, cultural, and organisational dynamics shape the everyday enactment of equal treatment in military life. This framework guides both the empirical design and the analytical interpretation of our findings in subsequent sections.

3. Legal-Institutional Framework and NATO Alignment

The Hungarian legal system has formally incorporated both domestic and international equality standards into its defence governance. Domestically, the Fundamental Law (Alaptörvény) guarantees equal treatment under Article XV, while Act CXXV of 2003 on Equal Treatment and the Promotion of Equal Opportunities (ETA) serves as the principal legislative tool to combat discrimination. These legal provisions apply to all public institutions, including the Hungarian Defence Forces (HDF), mandating internal procedures for addressing grievances and promoting equal access to military careers.

In addition to national law, Hungary is bound by international and transnational legal instruments. At the EU level, Directive 2000/43/EC and Directive 2000/78/EC establish legal frameworks against discrimination based on racial or ethnic origin and religion or belief, disability, age, or sexual orientation in the context of employment. These directives are binding on member states and require concrete institutional mechanisms, including equality bodies and complaint procedures. In the defence sector, these norms influence human resources policy, recruitment, promotion, and training processes.

From the NATO side, the most significant development is the 2022 NATO Strategic Concept, which reiterates member states' commitment to democratic values, gender equality, and inclusive security (NATO 2022). It explicitly states that "human rights, international law, and democratic institutions are essential to our Alliance." NATO also promotes the Women, Peace and Security (WPS) agenda, requiring member states to integrate gender perspectives into defence planning and operations.

Institutionally, the HDF has adopted formal mechanisms aligned with these standards. Equality officers are appointed at various command levels, and

procedures for handling discrimination complaints are in place. Nonetheless, the effectiveness of these mechanisms is often questioned. While formal policies exist, their implementation frequently lacks consistency, especially in rural and peripheral military units. There is limited evidence of systematic audits or impact assessments evaluating the success of these equality measures.

This fragmented implementation reflects broader tensions in the Hungarian public sector, where formal compliance with international norms is often prioritised over substantive transformation. Moreover, Hungary's evolving relationship with the EU and its ambiguous position within transatlantic governance sometimes complicate its alignment with NATO's normative expectations.
Thus, while the legal-institutional framework is robust on paper, its operationalisation within the military remains uneven, highlighting the need for stronger internal accountability, capacity building, and cultural change initiatives.

Defence institutions are embedded within a multilayered normative environment that encompasses universal human rights, humanitarian law, international strategic frameworks, and domestic statutes. This section maps the key legal and policy instruments that shape equal treatment commitments in the Hungarian Defence Forces (HDF), distinguishing between international, European Union, and national sources.

3.1. International Norms

At the international level, Hungary is bound by a range of instruments that promote equality and prohibit discrimination in military settings. These include:

- **United Nations Frameworks**: The Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW 1979) enshrine equality as a universal right. United Nations Security Council Resolution 1325 and its subsequent resolutions (2000–2022) further promote the inclusion of women in peace and security processes.
- **International Humanitarian Law (IHL)**: The 1949 Geneva Conventions and their 1977 Additional Protocols prohibit adverse distinctions in treatment, including during detention and the treatment of wounded soldiers (ICRC 2016).
- **NATO Frameworks**: NATO's Bi-Strategic Command Directive 40-1 on Gender Perspectives (rev. 2019) and its Policy on Preventing and Responding to Sexual Exploitation and Abuse (2019) establish zero-tolerance standards for harassment and require gender analysis in operational planning.

These international norms collectively provide a foundational commitment to equal treatment across armed forces, though their domestic implementation varies.

3.2. European Union Legal Framework

The European Union promotes equal treatment through a sophisticated regulatory framework encompassing primary law (e.g., the Charter of Fundamental Rights),

secondary legislation (Directives), and jurisprudence from the Court of Justice of the European Union (CJEU).

Key Directives

The most relevant EU directives include:

- **Directive 2000/43/EC (Race Equality Directive)** and **Directive 2000/78/EC (Framework Employment Directive)**: These prohibit discrimination in employment and vocational training based on racial or ethnic origin, religion, disability, sexual orientation, and age.
- **Directive 2006/54/EC (Gender Recast Directive)**: Consolidates gender equality provisions across employment and vocational contexts.
- **Directive 2010/41/EU** and **Directive 2019/1158/EU**: Address equal treatment for self-employed workers and promote work–life balance through parental leave and flexible working rights.
- **Directives 2024/1499 and 2024/1500**: Strengthen the institutional capacity of equality bodies and enhance enforcement mechanisms.

Jurisprudence

Seminal CJEU rulings further delineate the boundaries of equality in military settings:

- **Tanja Kreil (C-285/98)**: Held that excluding women from armed positions violates EU gender equality law.
- **Sirdar (C-273/97)** and **Schnorbus (C-79/99)**: Established that equal treatment is a fundamental social objective of EU law.
- **Alexander Dory (C-186/01)**: Recognised military service as a national prerogative but reaffirmed that professional service must respect equality principles.

Soft Law

Articles 21 and 23 of the **Charter of Fundamental Rights of the European Union** prohibit discrimination and promote gender equality. The **EU Gender Equality Strategy 2020–2025** encourages defence sectors to apply intersectional and inclusive approaches.

Application to Hungary

While EU law does not harmonise military recruitment, its equality directives apply to civilian personnel and, depending on national transposition, to military personnel as well. Hungary has transposed most relevant directives via **Act CXXV of 2003** and the **Government Decree 137/2024 (VI. 28.)**, reinforcing the legal obligation to uphold equal treatment in military service.

3.3. Domestic Legal and Policy Instruments

Hungary has developed a comprehensive legal and policy architecture to operationalise its equal treatment commitments:

The Fundamental Law of Hungary (2011), Article XV: Guarantees equality before the law and prohibits discrimination.
Act CXXV of 2003 (Equal Treatment Act): Applies universally, including the Ministry of Defence and HDF; establishes the Equal Treatment Authority to investigate complaints.
Act CCV of 2012 (Military Service Act): Explicitly prohibits discrimination in all phases of military employment.
Government Decree 1035/2021: Implements Hungary's second National Action Plan on Women, Peace and Security under UNSCR 1325.
Ministry of Defence Order 29/2022 (HR): Introduces practical measures, including awareness training, mentoring, and diversity reporting.
Chief of Defence Staff Directive 13/2023: Provides internal mechanisms for complaints and whistleblower protection.

3.4. Enforcement and Oversight Mechanisms

TABLE NO. 1

Enforcement and Oversight Mechanisms

Mechanism	Scope	Monitoring Body
Equality Impact Assessments	All new MoD policies and operational orders	MoD Human Resources Directorate
Annual Diversity Report	Workforce data, promotion outcomes, and disciplinary trends	Joint review by HR Directorate and Military Intelligence
Complaints & Redress	Individual grievances	Equal Treatment Authority; Military Ombudsperson

Source: compiled by the author

Despite the formal robustness of these frameworks, qualitative interviews reveal gaps in enforcement, particularly at the field level. Many personnel members report a lack of awareness regarding their rights under the Equal Treatment Act, and fear that filing a complaint could harm their career prospects. These patterns align with previous findings on post-socialist military cultures, where informal hierarchies may override formal safeguards (Szvircsev-Tresch 2014).

3.5. Interim Assessment

Hungary's defence sector is formally embedded in a dense and layered system of international, European, and domestic obligations aimed at guaranteeing equal treatment. However, the institutional translation of these norms remains uneven. Legal frameworks alone are insufficient to produce equality unless accompanied by cultural change, leadership commitment, and institutional learning.

The next section presents the qualitative methodology used to examine how these normative frameworks are internalised or resisted within the Hungarian Defence Forces.

4. Methodology

This study adopts a qualitative, institutionally grounded case study design to explore how equality norms are translated into military practice within the Hungarian Defence Forces (HDF). The aim is not to measure compliance in a statistical sense, but to understand the organisational and cultural dynamics that shape normative implementation.

4.1. Research Design

The study adopts a constructivist epistemological stance, acknowledging that organisational realities are socially constructed by actors within the defence sector. An exploratory case study approach was selected, focusing specifically on the Hungarian Defence Forces (HDF), while situating the analysis within a broader comparative frame of NATO member states. The units of analysis encompassed three interconnected domains: policy documents, organisational processes, and the individual experiences of service personnel. This design enables a contextualised understanding of how equality norms are translated into practice, drawing attention to both the formal regulatory frameworks and the informal dynamics that shape implementation on the ground.

4.2. Data Collection

A multi-method research design was employed to capture both formal frameworks and lived experiences within the Hungarian Defence Forces (HDF). The study combined document analysis of national legislation, NATO and EU directives, and internal HDF regulations with semi-structured interviews conducted with 18 current and former personnel, including officers, administrative staff, and equality officers from various regions. In addition, field observations and organisational mapping were conducted, focusing on procedures related to recruitment, grievance handling, and promotion. Two focus groups with junior enlisted women were held to explore intersectional dynamics in everyday military life. Finally, training materials – particularly diversity and inclusion (D&I) modules and their participant evaluations – were reviewed to assess the pedagogical and institutional approach to equality training.

TABLE NO. 2

Data source

Mechanism	Scope	Monitoring Body
Equality Impact Assessments	All new MoD policies and operational orders	MoD Human Resources Directorate
Annual Diversity Report	Workforce data, promotion outcomes, and disciplinary trends	Joint review by HR Directorate and Military Intelligence
Complaints & Redress	Individual grievances	Equal Treatment Authority; Military Ombudsperson

Source: compiled by the author

Participants were selected through purposive and snowball sampling to ensure variation in rank, branch, geographical posting, and gender identity, thus enabling a comprehensive account of both systemic practices and individual perceptions.
All interviews and focus groups were audio-recorded (45–75 minutes) and transcribed verbatim. Transcripts were anonymised, with pseudonyms used in analysis and reporting.

4.3. Data Analysis

The analysis followed a directed content approach (Mayring 2014), combining deductive coding based on the conceptual framework with inductive refinement grounded in participant narratives. Thematic analysis was conducted using MAXQDA 24 (Braun and Clarke 2006), with initial codes derived from pre-established categories such as rule interpretation, institutional culture, procedural fairness, and leadership influence. To ensure reliability, 15% of the interview transcripts were double-coded by an independent researcher, yielding a Cohen's κ of 0.82, which indicates substantial inter-coder agreement. Triangulation was employed by cross-validating themes across interview data, policy documents, and field observations, enhancing the robustness and credibility of findings (Guest, Namey and Mitchell 2013).

Throughout the research process, reflexivity was carefully maintained. The lead researcher's prior involvement as a trainer in defence-sector equality programmes offered valuable contextual understanding, while also necessitating critical self-awareness regarding their own positionality and potential interpretive biases (Berger 2015).

4.4. Trustworthiness and Limitations

While triangulation and a robust audit trail contributed to the methodological rigour of this study, several limitations must be acknowledged. S**election bias** may have occurred, as voluntary participation could have led to an overrepresentation of personnel with favourable views on inclusion or prior engagement with equality initiatives. R**estricted access to classified operational documents** limited the depth of insight into real-time implementation practices, particularly in active deployment contexts. The **cross-sectional nature** of the study constrains causal inference; longitudinal designs would be more suitable for capturing institutional change over time and assessing the durability of interventions.

Finally, while gender, ethnicity, and class were central to the analytical framework, voices related to **sexual orientation and disability** were underrepresented, pointing to the need for future studies to adopt more inclusive sampling strategies.

4.5. Ethical Considerations

All phases of the research adhered to rigorous ethical standards, in line with both national regulations and international best practices in social science research. **Ethical approval** for the study was granted by the Hungarian Defence Forces

Research Ethics Committee (Ref. HDF 2024/07). Prior to participation, all individuals provided **written informed consent**, having been clearly informed of the study's aims, their voluntary involvement, and their right to withdraw at any point without any adverse consequences. To ensure **confidentiality**, all personal identifiers were removed during transcription and analysis, and the data were stored on encrypted servers accessible only to the authorised research team.
These measures were essential in building trust with participants, particularly given the hierarchical nature of military institutions and the sensitivity of equality-related topics.

5. Case Study: Integration of Women in the Hungarian Defence Forces

Empirical Findings and Thematic Analysis The empirical data reveal a complex picture of how equality norms are implemented – or bypassed – in the Hungarian Defence Forces (HDF). Four interlocking themes emerged during the analysis: (1) organisational culture and leadership, (2) procedural inequality and complaints, (3) spatial disparities in implementation, and (4) compliance infrastructure and institutional resistance.

5.1. Organisational Culture and Leadership Commitment

Many interviewees reported that the commitment of local commanders plays a decisive role in whether equal treatment policies are effectively implemented. In units where leadership actively supports inclusion, equality initiatives tend to be more visible, and staff feel safer to raise concerns. Conversely, in hierarchically rigid or traditionalist environments, equal treatment policies are often viewed as formalities with little bearing on everyday military life. Some respondents noted that female personnel continue to face implicit expectations to conform to masculine behavioural norms, especially in combat or command-track roles.

5.2. Procedural Inequality and Complaint Mechanisms

While formal procedures for reporting discrimination exist, many interviewees expressed scepticism about their effectiveness. Several described the complaint channels as bureaucratic, opaque, or prone to retaliation. In some cases, informal social hierarchies discouraged personnel from reporting unequal treatment, especially when the perpetrator was a superior officer. Despite institutional efforts to train equality officers, their visibility and trustworthiness varied considerably between units. This suggests that procedural equality cannot be achieved solely through policy design – it requires legitimacy and enforcement capacity at the unit level.

5.3. Spatial Disparities in Implementation

Spatial inequalities emerged as a salient feature in the data. Units located in central or urban areas tended to have better awareness of equal treatment norms and more proactive leadership. In contrast, peripheral or rural garrisons displayed greater inertia

and less familiarity with compliance expectations. This divide reflects broader patterns in Hungarian public administration, where institutional innovation often concentrates in Budapest while rural areas lag in procedural reform and rights-based training.

5.4. Compliance Infrastructure and Institutional Resistance

The institutionalisation of equality within the HDF remains uneven. Although equality officers are formally appointed and HR procedures reflect legal requirements, their impact is often limited by competing institutional logics – namely loyalty, command, and cohesion. Some interviewees described equality policies as "paper compliance," suggesting a gap between formal alignment and internalised organisational change. Moreover, the lack of systematic evaluation or benchmarking mechanisms makes it difficult to track progress or hold units accountable.

5.5. Historical Background

The integration of women into the Hungarian Defence Forces (HDF) dates back to 1996, when the first cohort of female cadets entered the National Defence University (Zsoldos 2019). Hungary's accession to NATO in 1999 accelerated policy reforms, culminating in the 2000 amendment of the Military Service Act, which formally opened all non-combat positions to women. Full combat-role eligibility was introduced in 2013, mirroring the trajectory of several allied armed forces (Carreiras 2015).

5.6. Current Participation Snapshot

TABLE NO. 3

According to the HDF Human Resources Report 2023 (HDF HR Directorate 2024)

Mechanism	Scope	Monitoring Body
Equality Impact Assessments	All new MoD policies and operational orders	MoD Human Resources Directorate
Annual Diversity Report	Workforce data, promotion outcomes, and disciplinary trends	Joint review by HR Directorate and Military Intelligence
Complaints & Redress	Individual grievances	Equal Treatment Authority; Military Ombudsperson

Source: compiled by the author

While the overall share of women (≈10 %) aligns with regional peers (e.g., Poland 8 %, Slovakia 11 %), it remains below the NATO average of 12.2 % (NATO 2023).

5.7. Barriers to Integration

Interview data reveal four recurring obstacles:

1. Cultural Stereotypes – Persistent beliefs that combat effectiveness depends on 'traditional' gender roles create informal pressure on women to opt for support branches (Interview 08, female captain).
2. Work–Family Conflict – Limited on-base childcare and rigid deployment cycles disproportionately affect women, 73 % of whom self-identify as primary

caregivers (HDF HR Directorate 2024).
3. Mentorship Gap – Only 6 % of senior officer mentors are women, constraining career guidance for junior female personnel.
4. Harassment and Reporting – Although MoD Order 29/2022 mandates zero tolerance, 41 % of interviewees believe retaliation fears deter formal complaints (Interview 12, HR specialist), echoing NATO-wide surveys (Jackson 2021).

5.8. Enablers and Good Practices

A number of promising practices within the Hungarian Defence Forces illustrate the potential for institutional innovation when leadership support and targeted programming align. Since 2021, **Gender Focal Points (GFPs)** have been established at the brigade level to support gender-sensitive planning and act as confidential advisers, enhancing both operational awareness and trust in grievance handling mechanisms (GFP Network Report 2023). In parallel, the **Hybrid Deployment Model** piloted by the 25th Infantry Brigade, which allows for flexible 4 + 2-month rotations, has helped reduce family-related attrition and improve retention rates among women soldiers. Another notable initiative is the **'Forward Together' mentoring programme**, which pairs mid-grade women officers with senior leaders (colonels and brigadiers). This intervention has yielded measurable outcomes: a 28% increase in promotion rates among mentees within two years (MoD Evaluation 2023). Finally, the **STEM Scholarship Scheme,** aimed at female cadets at the Military Technical Faculty, has led to a twofold increase in enrolment in cyber defence specialisations since 2020 (Budai 2022).

These initiatives demonstrate that even within a traditionally hierarchical institution, well-designed and adequately resourced interventions can make measurable progress toward gender equality in military careers.

5.9. Comparative Insights

Compared with Canada's CAF and Norway's Armed Forces – often cited as gender integration pioneers – the HDF lags behind in three areas: (i) maternity/paternity leave parity; (ii) gender-disaggregated performance metrics; and (iii) leadership accountability for inclusion outcomes (Franklin 2018; Norwegian Ministry of Defence 2022).

However, Hungary's early adoption of GFPs at tactical levels represents an innovative practice not yet universal across NATO. The HDF has moved from formal equality (legal access) toward substantive equality (support structures), yet participation stagnates near 10 %. Structural barriers – especially caregiving burdens and limited mentorship – continue to constrain women's career progression.

The good practices identified offer scalable models but require strong leadership endorsement and sustained resourcing. These insights feed into the broader analysis of Section 6.

6. Conclusion and Policy Recommendations

This study has explored the institutional dynamics of equal treatment within the Hungarian Defence Forces (HDF), situated within the broader normative frameworks of the European Union and NATO. While Hungary has made formal commitments to non-discrimination and equal opportunity in defence, the translation of these norms into military practice remains fragmented and uneven.

The findings suggest that legal alignment alone is insufficient to ensure substantive equality. Organisational culture, leadership attitudes, spatial disparities, and weak enforcement mechanisms all contribute to a persistent gap between policy and practice. While some units demonstrate genuine efforts to embed equality values, others treat compliance as a bureaucratic obligation with limited practical implications.

The implications of these findings extend beyond Hungary. As NATO increasingly emphasises democratic resilience and inclusive security, member states are expected not only to adopt but also to internalise shared values. Hungary's case illustrates how the realisation of these values requires more than legal harmonisation – it necessitates a reorientation of institutional culture and leadership accountability.

Policy Recommendations

1. Strengthen Equality Leadership at the Unit Level
Appoint and empower equality officers with real authority and independence, ensuring they have the resources and training to operate effectively across all regions.

2. Establish External Monitoring and Benchmarking Mechanisms
Develop independent audit processes to assess the implementation of equality policies across units, with publicly available benchmarking indicators.

3. Incorporate Equality Criteria into Military Evaluations
Integrate equality performance into commander evaluations and promotion criteria to incentivise leadership engagement with these values.

4. Address Spatial Inequality through Targeted Interventions
Deploy additional resources and training programmes to rural and peripheral garrisons, ensuring that compliance is not geographically biased.

5. Enhance NATO–Member State Dialogue on Internal Compliance

Encourage NATO to offer more structured platforms for sharing best practices, technical assistance, and peer review in the area of military inclusion and human dignity. In conclusion, achieving normative equality in the military requires a holistic approach – one that combines legal obligation with institutional learning, leadership commitment, and cultural transformation.

7. Findings and Discussion

This section synthesises evidence from documents, interviews, and the case study to assess how far the Hungarian Defence Forces (HDF) have moved from formal commitments to substantive equality. Four interlocking themes emerge.

7.1. The Policy–Practice Gap Remains Pronounced

Despite a sophisticated legal–normative architecture (Section 3), implementation is uneven. Only 53 % of the 25 MoD policy texts analysed include an Equality Impact Assessment (EIA), although EIAs are mandatory under MoD Order 29/2022. Battalion-level commanders reported that EIAs are perceived as "paper exercises" due to limited guidance and time constraints (Interview 05, infantry colonel). This corroborates earlier findings on 'tick-box' compliance in Central and Eastern Europe (Anker 2020).

At the personnel level, interviewees identified knowledge gaps: 11 of 18 participants were unaware of the Equal Treatment Authority's remit. The absence of a robust dissemination strategy thus erodes the practical force of legal guarantees (De Feyter 2021).

7.2. Operational Consequences: Mission Effectiveness at Stake

Operational commanders highlighted three areas where limited diversity hinders performance:

1. **Human Intelligence (HUMINT):** All-female engagement teams remain ad hoc; opportunities to gather gender-sensitive information – especially in peacekeeping – are lost (Winslow and Dunn 2002).
2. **Retention Under Stress:** Units with higher female representation reported lower attrition during a 2022 peace-support deployment (internal after-action review, cit. Interview 03).
3. **Public Legitimacy:** Mixed-gender patrols received more favourable media coverage in Kosovo, enhancing strategic communication goals (HDF Press Report 2021).

These findings align with the 'business case' literature (Thomas and Ely 1996) that links diversity to organisational adaptability.

7.3. Leadership and Culture Shape Outcomes

Leadership commitment surfaced as the most powerful enabling factor. Units piloting the Gender Focal Point (GFP) model showed faster uptake of inclusion initiatives and lower harassment reports (GFP Network Report 2023). Conversely, two mechanised battalions lacking visible senior support recorded the highest incidence of "gendered microaggressions" in interview narratives.

Mentorship emerged as a critical but under-resourced mechanism. While the *Forward Together* programme boosted promotion rates among mentees (see Section 5), its reach remains limited to 40 % of eligible women officers. Expansion hinges on incentivising senior male officers to mentor across gender lines (Franklin 2018).

7.4. Toward an Inclusive Force: Necessary Conditions

Combining the above insights, four conditions appear essential to jump-start substantive equality within the Hungarian Defence Forces.

First, the introduction of **strategic performance metrics**, such as a Diversity Scorecard tied to commanders' annual evaluations, would embed inclusion into leadership accountability frameworks. This approach mirrors the Canadian Armed Forces' current practice (CAF 2023) and shifts inclusion from peripheral rhetoric to measurable leadership responsibility.

Second, a tangible **resource commitment** is necessary: earmarking at least 0.5 percent of the personnel budget for diversity and inclusion programming would bring Hungary in line with NATO frontrunners like Norway (Norwegian Ministry of Defence 2022). This financial allocation signals institutional seriousness and enables scalable interventions, such as mentoring schemes and tailored training modules.

Third, sustained **professional development** must be institutionalised. Embedding mandatory diversity and inclusion (D&I) modules into officer career courses – especially at the National University of Public Service – would normalise inclusion as a core leadership competency rather than a peripheral obligation.

Finally, **transparent accountability** through the annual publication of disaggregated personnel data – covering recruitment, promotion, and disciplinary outcomes – would not only enhance organisational trust but also enable evidence-based policymaking and public scrutiny. Such measures have proven effective in other NATO states seeking to bridge the gap between legal equality and lived inclusion (Jackson 2021).

Together, these four conditions form the backbone of a transformation strategy that moves beyond formalistic compliance, creating the organisational and cultural infrastructure necessary for durable equality. These conditions inform the policy recommendations in Section 8.

8. Policy Recommendations: From Formal Norms to Substantive Inclusion

This study has shown that, despite legal and normative commitments, the practical implementation of equal treatment norms within the Hungarian Defence Forces (HDF) remains uneven and fragmented. To bridge the persistent policy–practice gap, a set of interrelated policy measures is required, grounded in international benchmarks and responsive to organisational realities.

First, a robust institutional governance and accountability framework should be established. This includes the development of a standardised Diversity and Inclusion

(D&I) performance scorecard that tracks not only gender representation but also disparities in promotion, complaint resolution, and training participation. These indicators should be reviewed annually and linked directly to the performance evaluation of unit commanders. Equality Impact Assessments (EIAs), which are mandated by MoD Order 29/2022, require methodological strengthening and formal oversight by the legal department of the Ministry of Defence (MoD). Transparency is essential; thus, the MoD should publish an annual defence equality report disaggregated by gender, rank, and regional command, mirroring international best practices (CAF 2023; Jackson 2021).

Second, budgetary allocation must reflect policy priorities. A minimum of 0.5 percent of the personnel budget should be ringfenced for D&I programming, consistent with leading NATO member states (Norwegian Ministry of Defence 2022). Funding should support mentoring programmes, multilingual recruitment materials, inclusive leadership training, and gender-sensitive infrastructure. The existing Gender Focal Point (GFP) network should be expanded to ensure that every brigade has at least one full-time, trained equality advisor. Family-friendly service conditions must also be extended, including flexible deployment cycles and on-base childcare services. The effectiveness of these measures should be monitored through uptake rates and exit interview analysis.

Third, organisational culture change is essential. Inclusive leadership modules should be institutionalised within officer education at the National University of Public Service and embedded in promotion-track training courses. These modules must address unconscious bias, inclusive team dynamics, and conflict mediation. Cross-gender mentoring should be incentivised, with senior male officers encouraged to mentor junior female personnel as part of career advancement criteria (Franklin 2018). Reverse mentoring pilot programmes may also sensitise senior leadership to the lived experiences of underrepresented personnel. Additionally, peer-led inclusion workshops facilitated by trained non-commissioned officers (NCOs) could provide practical engagement with topics such as respectful communication, microaggressions, and bystander intervention.

Fourth, Hungary's integration into NATO's equality governance architecture should be deepened. The HDF should align with NATO's Gender Equality Baseline Assessment (GEBA) indicators and report progress to the NATO Committee on Gender Perspectives on a biennial basis. Bilateral learning exchanges with allied militaries – particularly the Canadian Armed Forces (CAF) and the Norwegian Armed Forces – could facilitate knowledge transfer in areas such as inclusive leadership, gender-disaggregated metrics, and accountability mechanisms.

Finally, Hungary could play a leading role within NATO by advocating for spatial disaggregation of inclusion metrics, recognising that regional inequalities directly affect alliance cohesion and operational legitimacy (De Feyter 2021; Soja 2010).

These recommendations are not only feasible within the existing institutional framework but also urgent in light of the operational and normative challenges identified in this study. Substantive equality in defence cannot be achieved through legalism alone; it requires cultural commitment, resourced mechanisms, and territorial sensitivity.

References

Berger, R. 2015. "Now I see it, now I don't: Researcher's position and reflexivity in qualitative research." *Qualitative Research* 15 (2): 219–234. https://doi.org/10.1177/1468794112468475.

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

CAF. 2023. *Canadian Armed Forces Diversity and Inclusion Annual Report 2022–2023.* Ottawa: Department of National Defence.

Carreiras, H. 2015. "Gender and civil–military relations in advanced democracies." *Res Militaris* 1 (1): 1-18.

___. 2006. *Gender and the military: Women in the armed forces of Western democracies.* 1st ed. Routledge. https://doi.org/10.4324/9780203969038.

CEDAW. 1979. *Convention on the Elimination of All Forms of Discrimination against Women.* New York: United Nations General Assembly.

Clomax, A.J., M.E. Mor Barak, A.M. Hancock, J. Dodge, S. Kintzle, R. Cox, and C. Castro. 2024. "An intersectional analysis of women's experiences of inclusion in the United States Army." *Sex Roles* 90 (11): 1666–1680. https://doi.org/10.1007/s11199-024-01524-8.

De Feyter, K. 2021. *Globalization and the common responsibilities of states.* Routledge.

Demeter, F. 2022. "Regionális és társadalmi különbségek a katonai pályaorientációban." *Honvédségi Szemle* 151 (2): 53-68. https://doi.org/10.35926/HSZ.2022.2.5.

Franklin, C. 2018. "Gender, mentorship and organisational change in defence institutions." *International Journal of Security Studies* 12 (1): 55–72.

Guest, G., E.E. Namey, and M.L. Mitchell. 2013. *2013. Collecting qualitative data: A field manual for applied research.* Los Angeles: Sage. https://doi.org/10.4135/9781506374680.

International Committee of the Red Cross (ICRC). 2016. *Advancement of women: ICRC statement to the United Nations.* Geneva: ICRC.

Jackson, M. 2021. *Gender integration in NATO forces: Assessment and accountability.* NATO Research Division.

Makkos, N. 2024. "Egyenlő bánásmód a hadseregben (vázlat)." *Honvédségi Szemle* 152 (3): 99–112. https://doi.org/10.32563/hsz.2024.3.8.

Mayring, P. 2014. *Qualitative content analysis: Theoretical foundation, basic procedures and software solution.* Klagenfurt: Beltz.

National Assembly of Hungary. 2003. "Act CXXV of 22 December 2003 on equal treatment and promotion of equal opportunities." Budapest.

Ni Aoláin, F., D.F. Haynes, and N. Cahn. 2011. *On the frontlines: Gender, war, and the post-conflict process.* Oxford University Press.

Norwegian Ministry of Defence. 2022. *Equality, diversity and inclusion in the Norwegian Armed Forces.* Oslo: Government of Norway.

Soja, E.W. 2010. *Seeking spatial justice.* University of Minnesota Press. https://doi.org/10.5749/minnesota/9780816666676.001.0001.

Thomas, D.A., and R. Ely. 1996. "Making differences matter: A new paradigm for managing diversity." *Harvard Business Review* 74 (5): 79-90.

True, J. 2016. "Explaining the global diffusion of the Women, Peace and Security agenda." *International Political Science Review* 37 (3): 307–323. https://doi.org/10.1177/0192512116639512.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Governing International Private Security Companies: Conceptual Contours, Normative Debates, and Strategic Divergences

Kuang-Ho YEH, PhD*

*Graduate School of International Studies and Regional Development
University of Niigata Prefecture, Japan
e-mail: ry1207@gmail.com

Abstract

The rise of international Private Security Companies (PSCs) has drawn scholarly attention in security studies. Academic inquiry has shifted from early debates on legality and implications to theoretical and empirical analyses of governance mechanisms. Comparative studies identify distinct governance typologies: state-integrated, market-driven, and deficiency models. To explain this variation, this article proposes a bivariate framework based on governance capacity and willingness. States with high capacity and strong political intent impose strict governance; those with strong capacity but limited willingness pursue moderate approaches; while strong willingness but weak capacity often results in absent governance. Through case studies of the United States, China, and the selective Global South state, the analysis demonstrates considerable explanatory power. Theoretically, it links governance variation to structural determinants; empirically, it reveals how governance preferences stratify along lines of developmental disparities. Achieving effective international PSC governance requires synergistic efforts via acknowledging national regulatory comfort zones to identify common ground for shared norms, multilateral agreements, and binding international legal frameworks.

Keywords:
International Private Security Company; Normative Legitimacy; Regime Maturity; Governance Capacity; Governance Willingness; Global South.

Article info
Received: 12 August 2025; Revised: 1 September 2025; Accepted: 11 September 2025; Available online: 6 October 2025

Citation: Yeh, K.H 2025. "Governing International Private Security Companies: Conceptual Contours, Normative Debates, and Strategic Divergences". *Bulletin of "Carol I" National Defence University*, 14(3): 185-207. https://doi.org/10.53477/2284-9378-25-43

Private Security Companies (PSCs) have emerged as prominent non-state actors in international relations in the post–Cold War era. To date, their growing relevance has been increasingly acknowledged. As PSCs' activities evolve, scholarly attention has shifted toward examining how governance[1] can further consolidate their legal foundations and ensure effective oversight. However, the construction of legitimacy through impactful governance pathways remains challenged. For international PSCs to achieve sustainable development and broader recognition, they must not only adapt to existing governance architecture to enhance institutional compatibility, but also account for the pivotal role of sovereign states—core actors in international politics—in shaping development outcomes through material capacities and governance agency. State actors exhibit considerable heterogeneity in their approaches to governing PSCs: some countries utilize embedded governance models, while others adopt defensive governance strategies. Unpacking the mechanisms behind these divergent trajectories provides both a conceptual framework for anticipating future developments in private security sectors and a generalizable explanation for the governance barriers facing emerging international actors.

Driven by problem awareness, this article employs the following research design: it reviews existing literature to identify limitations of prevailing paradigms concerning PSCs' ontology and governance. Second, it constructs a dual-dialectical framework centered on security governance demand: state governance capacity and willingness. Third, it conducts a comparative analysis of representative cases among a developed country, a major developing power, and a Global South state, culminating in a theoretical model of differentiated governance to guide the concluding synthesis.

1. International PSCs: Brief Delineation of Research Subject

International PSCs are legally registered entities operating under market mechanisms with the objective of capital accumulation. They provide services to a variety of international actors, encompassing quasi-military[2] and military functions like combat and operational support, military consulting and personnel training, arms procurement, logistics, security services, intelligence collection, and crime prevention (Ortiz 2010). According to Singer (2004), PSCs can be classified based on the level of combat involvement and use of force into three categories: (1) Military-Provider Companies—directly engage in frontline operations and exercise force; (2) Military-Consultant Companies—offer strategic advice and personnel training, with limited force involvement; (3) Military-Support Companies—provide non-combat logistics such as transport, resupply, and infrastructure. Amid diversifying and de-territorialized global threats,

[1] Author's note: A terminological clarification is warranted. This article adopts governance, rather than government, as a deliberate conceptual choice. In standard usage, government denotes the office or authority that governs; governing refers to the act of ruling; and governance designates the ongoing activity of governing through which societal expectations are translated into collectively binding outcomes. Following Rosenau, governance is analytically far-reaching than government: whereas government connotes hierarchical rule and control, governance captures the broader orchestration and management of publicly relevant affairs by constellations of formal and informal actors. In this sense, governance foregrounds management, networks, and process over solely command. (Refer to: Fasenfest, David. 2010. "Government, Governing, and Governance." Critical Sociology 36(6): 771-774; Rosenau, James, and E.O. Czempiel. 1992. Governance without Government: Order and Change in World Politics. Cambridge University Press.)

[2] Paramilitary refers to organizations or units structured along military lines but operating outside the framework of formal armed forces, including armed nonstate actors and state-affiliated groups employed for coercion, enforcement, or local security. Often, paramilitary forces serve to consolidate political power or bolster authoritarian regimes.

PSCs have evolved from mere suppliers of force-related services into comprehensive security solution providers.

Max Weber defined the modern nation-state by its monopoly on the legitimate use of physical force—entailing the authorization, regulation, and exercise of violence (Weber 1964). However, historical evidence suggests that state exclusivity over military force is a contextual exception rather than a universal norm; private military actors distinct from regular armies have coexisted with warfare. In ancient Rome, India, and China, military organizations routinely relied on contracted troops to supplement state forces, highlighting the institutional embedding of private actors within national military systems. In the early modern period, from the Thirty Years' War to Victorian era colonial expansion, private actors not only participated in the battlefield but also contributed structurally to the European statehood and military institutions (Singer 2002). During the third wave of decolonization, large-scale mercenary activity was witnessed in the Global South, such as Fifth Commando and Operation Azalee, led by former European military personnel, which built the "lone wolf" image in Africa (Rookes and Bruyère-Ostells 2021). They were motivated by individual economic interests, with remuneration provided by conflict parties. Although mercenaries may provide an immediate augmentation of military capacity, the profit-driven nature and the attendant destruction inflicted upon conflict-affected communities frequently generate ethical stigma and involve illicit practices. Contemporary experiences demonstrate not only the objective functional distinctions between mercenary and the formally evolving private security industry, but also the necessity of clearly delineating them in subjective perception.

International legal Instruments such as the International Convention against Mercenaries and the First Additional Protocol to the Geneva Conventions deny mercenaries lawful combatant status (Vaux, et al. 2022). Consistently, the spirit of Article 47 of the First Protocol indicates that mercenaries are unprotected under the law of armed conflict and are not entitled to combatant or prisoner-of-war status. Owing to a lack of legal safeguards and their de facto illegitimate standing, mercenaries possess weak incentives to comply with international law, potentially triggering a negative feedback loop of humanitarian risks (Beyani and Lilly 2001). Under the architecture of international law, the UN discourse has shifted focus from the identity of actors to the nature of their activities, emphasizing institutionalization, accountability, and structural legitimacy extending to the governance domain of the superstructure, differentiating PSCs from mercenaries (Krahmann 2012). The modern international security industry underwent a systematic transformation in the post–Cold War 1990s. Escalating concerns over human rights violations, the dissemination of wartime casualties through media channels, and domestic opposition to foreign interventions led Western states to become reluctant to engage directly in regional conflicts (Hammes 2010). In response, the outsourcing of armed forces has gained traction, signaling the emergence of PSCs operating under corporate structures as pivotal instruments of national security policy. The

extensive adoption of security contractors by Western states is driven by hybrid factors—the reduction of personnel casualties among armed forces, and the covert advancement of geopolitical interests in grey zones. Moreover, echoing the profit-driven characteristics of mercenaries, PSCs exhibit substantial incentive structures with performance-based compensation exceeding the attractiveness of equivalent rank military salaries. Accordingly, numerous senior US veterans have actively founded or joined international PSCs to participate in operations in Iraq and other regions, viewing such engagement as an economically advantageous alternative to re-enlistment in active service (Williamson 1991). The clientele of PSCs now extends beyond states to encompass international organizations, NGOs, media outlets, and multinational corporations. Even the UN employs PSCs in its peacekeeping missions.

Structural drivers are underpinning this evolution. As major powers strategically retreat from the Global South, leaving security vacuums, the neoliberal turn in global governance has facilitated the use of PSCs to enhance military force through the provision of specialized skills and resources. This enables the filling of capacity gaps, ensures operational flexibility, and provides strategic advantages in conflicts requiring rapid response (Jefferies 2002). The shift also reflects a broader trend of security privatization, with PSCs increasingly integrating with infrastructure, information technology, telecommunications, and intelligence sectors. Gwatiwa (2016) emphasizes that PSCs are critical to defense policy formulation, allowing governments to assess the risks and benefits of outsourcing operations, balance security requirements against potential vulnerabilities, and make informed decisions regarding PSCs engagement.

2. Core Research Issues

As non-state actors performing security-related functions, PSCs operate outside the traditional paradigm of state monopoly on the use of force. Their profit-driven nature also creates principal-agent problems, leading to systemic violations of international humanitarian law. Thus, governance debates fall along a strategic spectrum of dominant conceptions. "Total prohibition" calls for re-nationalization of all military and security functions, reaffirming the doctrine of force monopoly, but overlooking the complex reality of PSCs' embedded role. Conversely, "market regulation" is grounded in neoliberal assumptions of self-regulation through the invisible hand, but neglects security market failures, including information asymmetry and moral hazard[3],revealing the inadequacy of market logic in deterring norm violations.

[3] Author's note: Private security companies complicate the traditional moral-ethical foundations of armed conflict. States have historically justified warfare on political or moral grounds, such as sovereignty, liberation, or justice. By contrast, PSCs are primarily profit-driven. Their involvement therefore diverges: instead of embodying state-directed ideational purposes, PSCs function as corporate actors that commodify security. This renders their presence morally ambivalent—simultaneously filling capacity gaps but eroding legitimacy of operations.

2.1. From Regulation to Governance: Responses to International PSCs

International efforts to govern PSCs can be delineated into distinct phases. Early instruments such as the protocols to the Geneva Conventions and the 1989 UN Convention against the Recruitment, Use, Financing and Training of Mercenaries, emphasized governance needs but narrowly targeted mercenary activity, excluding the support-oriented, non-combat role of modern PSCs (DCAF 2016). A milestone came with the 2008 Montreux Document, endorsed by 59 states and non-state actors. It introduced a tripartite responsibility scaffolding—territorial, home, and contracting states—and differentiated combat from security functions with reference to applicable legal standards. Nonetheless, as a soft law design of voluntary guidelines, it lacks the mandatory character of treaty law, imposing no formal obligations, leading to a compliance gap in its recommended "best practice." (DeWinter-Schmitt 2017) In parallel, industry-led mechanisms have emerged to compensate for the limited enforceability amid rapid expansion. The British Association of Private Security Companies (BAPSC) and the International Stability Operations Association (ISOA) promote voluntary codes of conduct to standardized professional behavior (Joachim and Schneiker 2012). However, their sanctions are limited to membership revocation, lack coercive authority, and deterrent impact. Therefore, despite growing normative frameworks, meaningful governance still hinges on robust state-level intervention as an indispensable governance apparatus.

2.2. Categorizing National PSCs Governance Models

Governance frameworks for international PSCs manifest through normative and enforcement dimensions. Normatively, comprehensiveness depends on whether states have enacted dedicated legislation and whether legal provisions cover key regulatory elements. Enforcement reflects both objective operability—clarity, precision, and procedural completeness of provisions, and the subjective proactivity of enforcement actors. The interplay between normative design and implementation reveals broader governance radiation: robust frameworks with rigorous enforcement suggest norm-driven models, while weak legislation and lax oversight indicate permissive governance. Disjunctions may also emerge where comprehensive laws are offset by poor implementation, or minimal legislation coexists with stringent enforcement commitment. This article adopts a governance-centered analytical lens emphasizing the theoretical rationales: the logic of legitimacy prioritizing legal conformity, and the logic of consequentiality emphasizing practical outcomes. States typically seek a dynamic equilibrium, resulting in approaches to international PSCs governance that can be categorized into the following typologies.

The first category, represented by the developed countries, is characterized by sophisticated institutional design paired with lax enforcement tendency and broad judicial discretion—here defined as "moderate governance." The United States exemplifies the model through a multifaceted legal and institutional system regulating international PSCs. The Arms Export Control Act (AECA) establishes a licensing regime governing the export of weapons and military services. The

Alien Tort Statute (ATS) and the Military Extraterritorial Jurisdiction Act (MEJA) provide legal grounds to hold PSCs accountable for unlawful acts committed abroad (Ryngaert 2008). Moreover, federal criminal law prohibits American citizens from providing military assistance to foreign governments at peace with the US, constraining extraterritorial conduct (Schreier and Caparini 2005). Given the operational complexity of PSCs, administrative and judicial actors retain considerable interpretative discretion, resulting in inconsistencies and regulatory ambiguity, particularly in transnational contractual execution and asymmetric conflict zones. A deep interest symbiosis between PSCs and government agencies, illustrated by the CIA's "shadow contractor" programs, has contributed to regulatory capture (Clanahan 2013). The prevalence of a reactive enforcement with accountability triggered only under intense public scrutiny, as exemplified by the 2007 Blackwater Baghdad shooting, is quintessential (Chen 2009). Although four employees were eventually convicted, the Trump administration pardoned them, granting immunity in 2020. This episode not only underscores the symbolic nature of accountability but can also be viewed as the military-industrial complex permeates political decision-making (Baum and McGahan 2009). The intermediary position—neither fully permissive nor strictly regulated—encapsulates the essential attributes of moderate governance.

The second category exemplified by emerging developing powers is defined as "strict governance". While comprehensive legal systems are under development, these states exercise intensive oversight of PSCs through adaptable administrative regulations. The promulgation of the 2009 Regulation on the Administration of Security Services (保安服务管理条例) marked the first specialized administrative regulation for Chinese PSCs. In 2010, the Ministry of Public Security issued the Measures for the Implementation of the Regulations on the Administration of Security Services by Public Security Organs (公安机关实施保安管理条例办法), elaborating regulatory scope and strengthening administrative control. Nonetheless, the applicability remains largely confined to domestic operations with limited efficacy over transnational PSCs activities. The public security authorities serve as the principal regulatory body supervising overseas PSCs through qualification assessments and licensing procedures. The authorization to bear arms constitutes the distinguishing feature of international PSCs (Drew and Mclaughlin 2016). In many conflict-affected developing countries and regions, international PSCs have served as key channels and intermediaries for the broker and transport of small arms and light weapons (SALW), thereby facilitating their proliferation and misuse (Makki, et al. 2001). Conversely, as the core component of the corporate qualification review system, China imposes stringent control on firearms use by PSC personnel, shaping the operational trajectory of Chinese international PSCs, predominantly toward the defensive and non-combat security service model (Pereira, et al. 2023).

The third category, "absent governance," characterizes weak developing countries in the Global South that commonly face the dilemma in governing international

PSCs due to underdeveloped regulatory systems and limited enforcement capacity. International PSCs in Afghanistan vividly illustrate the tension in post-conflict settings. Following the Taliban's collapse, the influx of international actors led to a hybrid security market where PSCs assumed both quasi-military and conventional roles, filling the security void while complicating the national security configuration. The proliferation of PSCs disrupted the disarmament, demobilization, and reintegration (DDR) efforts for ex-combatants and raised human rights concerns. The government prompted the centralization reform through the creation of the Afghan Public Protection Force (APPF) in 2010. However, the APPF blurred lines of responsibility as a hybrid public–private entity operating in a fragile institutional context (Bali, et al. 2024). Correspondingly, in Latin America and the Caribbean, high crime rates pose an enduring difficulty to security governance. PSCs have ostensibly been introduced to supplement weak public security against criminality. In Trinidad and Tobago, law enforcement agencies have struggled to curb escalating violence, fueling widespread public insecurity. Compounded with early military retirements since the 1980s has contributed to a surplus labor pool. To address these challenges, the government enacted the Supplemental Police Act and adopted the International Code of Conduct for Private Security Service Providers (ICoC). In 2010, a dedicated governance body—the Private Security Network Commission (PSNC)—was created to monitor the PSCs. Despite nascent efforts, the continued proliferation of PSCs amid limited public security improvements highlights the ineffectiveness of "triadic" collaboration among the state, private sector, and civil society, and has yet to realize its envisioned integration and operational coherence (Anyanwu 2012).

Through a comparative discussion of the aforementioned categories, it is observed that states exhibit substantial variation in governing international PSCs as strategic instruments for advancing national interests. However, a key theoretical puzzle arises: despite the widespread international recognition of PSCs' de facto legitimacy, as well as the path-dependent and paradigmatic emulation of security policymaking nature, why do national governance policies and their implementation still display marked divergence? Whether additional latent variables exist therein, or whether cross-variable chemical synergy transcends phenomenological observations? To systematically address this inquiry, the article begins with a critical review and theoretical synthesis of existing literature and maps an integrated analytical framework to guide subsequent empirical investigation.

3. Review of Intellectual Landscape

Current research on the governance of international PSCs coalesces around two primary clusters. The first pertains to empirical investigations of governance praxis adopted by state actors and the comparison of cross-national policy variations. Boddi et al. (2016) conducted some research on how contractual design and oversight mechanisms in outsourcing and procurement shape the behavioral constraints imposed on PSCs. Kruck (2020) explores the state's dual imperative of

capacity and control, arguing that governance complexity arises from the interplay between functional limitations and legitimacy concerns. In governance typologies, Button (2007) developed a binary model distinguishing between highly regulated accountability structures in continental Europe and minimal compliance governance favored in Anglo-Saxon countries. Leander underscores how Global South regimes deploy PSCs as instruments of authoritarian consolidation, with the civil–military–PSC nexus offering insight into the political interactions underlying such regimes. In contrast, Krahmann's comparative study of European countries identified the Public-Private Collaboration, encompassing hybrid governance arrangements such as defense contracting, joint ventures, and public equity participation; and the State Regulatory Mechanism encompassing the transnational provision of PSCs, such as the International Traffic in Arms Regulations (ITAR), by means of licensing procedures and compliance oversight (Krahmann 2005).

At the normative level, Cockayne and Mears (2009) propose a global governance framework based on quadripartite collaboration, comprising a Global Watchdog, Accreditation Regime, Arbitral Tribunal, Harmonization Scheme, and a Global Security Industry Club. Stinnett (2005) advocates a coordinated approach spearheaded by key states, underpinned by regulatory regimes like the US Arms Export Control Act (AECA), extending domestic jurisdiction extraterritorially to govern international contracts and mandate transparency. Saner et al. (2019) contend that the prevailing political ambiguity surrounding PSCs undermines the governance effectiveness of warfare in the public sphere. They propose the hybrid network combining binding mechanisms with soft law instruments, supplemented by strategic financial leverage.

However, existing research on the driving forces behind state policies toward governing international PSCs remains fragmented, lacking a coherent thematic scheme. States exhibit divergent policy logics and normative orientations. In the US, humanitarian concerns constitute a primary motivation for PSC governance, whereas Global South countries often prioritize sovereignty and regime preservation. There are two main analytical perspectives that dominate this discourse. The structuralist perspective highlights the constraining influence of global governance norms, such as the Montreux Document, on national policies. However, its explanatory power is limited by the voluntary and declaratory nature of existing norms, their shortness of enforceability, and geographic concentration undermines global inclusivity and operational specificity. The unitary state perspective emphasizes the role of domestic political, economic, and security contexts in shaping national governance approaches. While this view offers valuable case-based findings, it is constrained by methodological particularism. Most studies exhibit a Western-centric bias, reducing the external validity of their conclusions and failing to capture the full diversity of state behaviors.

Thus, this article aims to develop an innovative explanatory framework that integrates the considerate factors through a multivariable analytical approach. The objective is

to construct a robust theoretical tool capable of accounting for both cross-national variation and longitudinal shifts in PSC governance, addressing critical vacuums in the existing literature of the field.

4. Hypothesis and Analytical Framework

This article presents the argument that a state's choices in governing international PSCs fundamentally hinge on its governance capacity and governance willingness. The former provides the necessary administrative and institutional conditions for policy implementation, while the latter offers the motivational basis regarding both strategic intent for governance policy adoptions, and normative commitment for regulatory actions. Cross-national variation in PSCs governance reveals a patterned spectrum stemming from different combinations and intensities of these two dimensions. Building on this perspective, the article advances the core hypothesis reframing state governance types toward international PSCs—moderate governance, strict governance, and absent governance—now determined by association-driven configurations of governance capacity and governance willingness. To substantiate this hypothesis, the analysis incorporates the attributes of the governing actor (the state) and the governed object (the activities of PSCs), providing a more nuanced conceptualization of the mutually-constructed governance capacity and governance willingness that pertain to the ideational realm. It further explores the logical relationship between these two dimensions and the resulting policy outcomes, and derives corresponding theoretical testable propositions from the hypothesis. The explanatory framework is visually represented in Figure 1.

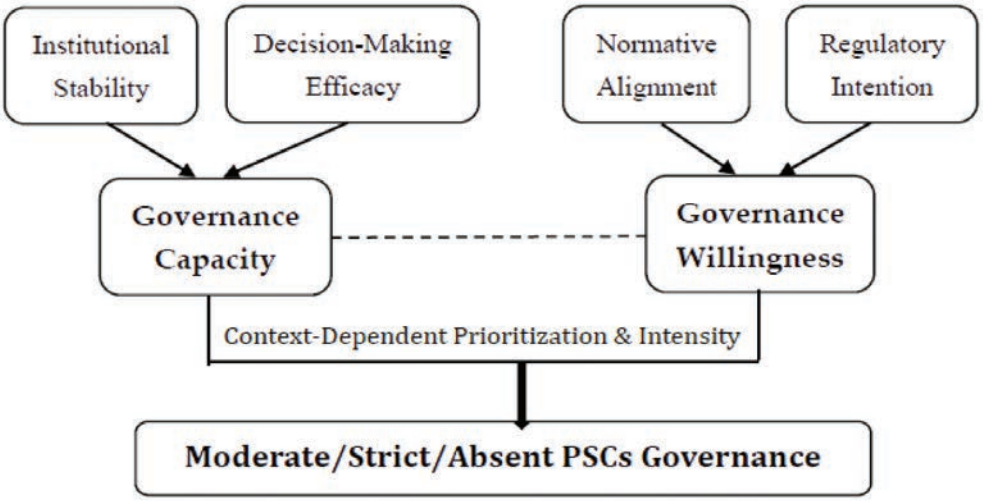

Figure 1 An Analytical Framework for Differentiated PSCs Governance Models
Source: own illustration

4.1. Governance Capacity

This article defines governance capacity as a state's comprehensive ability to regulate international PSCs under structural constraints to achieve its governance objectives. As a fundamental condition for policy implementation, governance capacity is

essentially determined by the core variable—regime maturity (Smith 1991), assessed through three key dimensions: (1) institutional stability measured by the degree of institutionalization in power transitions; (2) authoritative integration indicated by the coordination between central and local authorities; and (3) decision-making efficacy gauged by the institutionalization of interactions among political interest groups. High regime maturity ensures stable governance through a secure political environment, adequate policy resources, and efficient administrative execution. This conceptualization adheres to value neutrality, relying strictly on observable empirical indicators to minimize ideological bias.

Among these indicators, the institutionalization of regime change is particularly vital. While electoral mechanisms facilitate peaceful transitions, their effectiveness depends on each country's democratic trajectory and political culture. Extra-legal changes, such as coups or electoral manipulation, remain prevalent globally. Even consolidated democracies face risks. The 2021 Capitol Hill attack in the US exposed vulnerabilities in succession processes (Mourão and Brown 2025). Stable transitions underpin both policy continuity and institutional prerequisites for governance. Another critical dimension is the vertical configuration of political power. States are generally categorized into unitary, federal, or confederal systems. Unitary systems sustain policy uniformity but may suppress the agency of subnational units, while federal systems grant autonomy yet may face fragmentation challenges. A mature regime achieves a functional balance upholding centralized authority and local discretion. For states engaging with PSCs, political institutions directly shape governance capacity. National-level legal frameworks must be complemented by adaptable local implementation mechanisms. Finally, the political party system plays a crucial role in regime maturity. A well-functioning party system facilitating interest aggregation and government formation supports coherent policymaking (Novotný et al. 2016). Structured inter-party dynamics improve legislative efficiency and enhance policy continuity. In contrast, excessive partisan strife may lead to regulatory absence and fragmented enforcement. The procedural rationality and inclusiveness of party system are strongly correlated with the state's capacity and predictability in security governance.

4.2. Governance Willingness

Governance willingness refers to the normative and regulatory intent of a governing actor toward international PSCs, aiming at reinforcing their legitimacy in global security governance. It underpins the motivational foundation of governance actions. In other words, even robust governance capacity may result in inaction without such willingness. Although correlated with resource endowments, governance willingness is ultimately driven by value rationality—the alignment of policies with socially constructed norms and collective expectations. This concept parallels the logic of appropriateness in international relations, wherein actors prioritize normative conformity over instrumental calculation within a delimited geopolitical space to ensure legitimacy. International PSCs can be viewed as institutionalized

normative vehicles, reflected in two dimensions. At the organizational level, PSCs adopt modern corporate structures infused with Weberian bureaucratic systems, exhibiting formal-legal rationality and contract-based operational modalities. At the political-operational domain, their proliferation deconstructs the state-centric norm of monopoly over legitimate violence, reshaping authority in security governance across the public–private divide. From the perspective of the appropriateness logic, governance willingness is shaped by normative congruence (Nalbandov 2009)—the extent to which PSCs align with dominant norms of host states during transnational diffusion and interaction.

Normative congruence follows the localization logic, which posits that norm transmission is not a unidirectional "teaching" process but an agentic practice whereby recipient actors selectively adopt, reinterpret, and reconstruct external norms (Checkel 1999) in accordance with their preexisting normative frameworks. Effective internalization occurs only when norms resonate strategically with the domestic normative architecture at regional or local levels. In governing international PSCs, the diffusion of norms such as the Montreux Document can only elicit governance willingness if they: (1) interact constructively with sovereignty-based security governance; (2) integrate into existing public–private authority configurations; and (3) meet the legitimacy expectations of key domestic stakeholders (Buckland and Burdzy 2015). This adaptive process forms a negotiated normative order between global norms and local practices. A salient example lies in ASEAN's selective acceptance of European-exported PSC norms. While ASEAN successfully reconciled cooperative security norms aligned with its ASEAN Way, particularly the non-interference principle, it rejected Western-valued normative embraces such as humanitarian intervention. This divergence reflects the former's compatibility with ASEAN's political culture and deeper normative interests, whereas the latter stands in the incompatibility of regional foundations (Acharya 2004). Thus, when international norms on PSCs governance are transmitted domestically, their congruence with the target state's prevailing normative structures becomes a critical determinant influencing the effectiveness and the likelihood of institutionalization.

In sum, this article builds the governance willingness component chain based on the meta-theoretical premise that international PSCs function as institutionalized normative vehicles. It proposes the following causal mechanism: normative congruence (independent variable) → governance willingness (mediator) → governance policy choices and effectiveness (dependent variable). When PSCs-related norms exhibit structural isomorphism with the dominant normative architectures of the target state, a norm—willingness—action pathway is likely triggered. Conversely, lacking such congruence may provoke normative resistance, hindering governance outcomes.

4.3. Governance Capacity, Governance Willingness, and Strategic Choice

Approaches to governing international PSCs vary according to governance capacity and willingness. Based on the relative strength of these two dimensions,

four corresponding governance types can be identified (see Figure 2): (1) Strong capacity & strong willingness: States with well-developed institutional instruments and resources, coupled with clear strategic intent, tend to adopt strict governance (Module A), with China serving as a representative example. (2) Strong capacity & weak willingness: Some states possess robust legal infrastructure but lack sustained engagement due to interest-based trade-offs or competing ideational priorities. This results in moderate governance (Module C), as the US illustrates this pattern. (3) Weak capacity & strong willingness: States with limited institutional strength but high motivation, driven by domestic stability concerns or sovereignty pressures, struggle to implement effective oversight, leading to absent governance (Module B), a common picture observed among Global South countries. Sierra Leone exemplifies a salient theme where the fragmented authority, political decay, and elite networks shape the interconnectedness between PSCs and host governments. These dynamics reflect broader Global South trends: foreign leverage over natural resources, contested legitimacy, and non-state security proliferation. Finally, the theoretical scenario of weak capacity & weak willingness lacks empirical evidence in the current context in international politics and is therefore excluded from analysis.

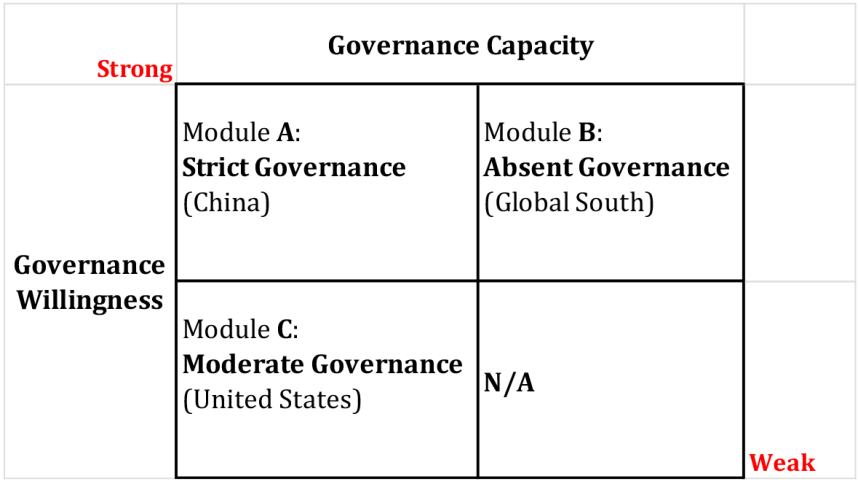

Figure 2 **The Matrix of Governance Capacity, Willingness, and Strategic Choices**
Source: own illustration

5. Case Studies

According to the report from the Stockholm International Peace Research Institute (SIPRI), the term "private security sector" is often a misnomer in weak or failed states. In such realities, reliance on private actors arises not from functional market dynamics but from the absence of effective national security governance. Often, no viable socio-economic foundation exists to support meaningful security privatization, contrasting sharply with strong or "efficient" states, wherein private security complements effective governance (Holmqvist 2005). Beyond objective material conditions, the state's normative perception of private security governance

constitutes a subjective factor shaping its strategic decision-making. The interplay between structural capacity and ideational orientation underpins the diverse governance strategies states adopt toward international PSCs.

5.1. Moderate Governance: The United States

The US private security industry is highly developed, encompassing services from information security to crisis management, and rivals the public police system in scale. On the international stage, US-based PSCs operate in numerous conflict zones, providing military training, intelligence, logistics, and protection for leaders of failed states. Despite scale and adaptability, the governance of US PSCs has been plagued by regulatory fragmentation and disciplinary laxity, repeatedly sparking humanitarian controversies and drawing global criticism.

5.1.1. Strong Governance Capacity

The United States possesses robust institutional capacity and regulatory expertise in governing international PSCs. Legally, federal statutes such as the AECA, International Traffic in Arms Regulations (ITAR), and National Defense Authorization Act (NDAA) define and constrain PSCs' activities regarding armament, personnel deployment, service scope, and foreign cooperation (Elsea 2010). Congressional oversight apparatus through budgetary review, investigative reports, and dedicated bodies like the Government Accountability Office (GAO) and the Department of Defense Office of Inspector General (DoD OIG) enhance transparency and accountability. Administratively, the Department of Defense and the Department of State oversee contract approvals, monitor implementation, and conduct risk assessments. During the Iraq and Afghanistan wars and reconstruction periods, the US developed classification systems distinguishing core, non-core, and intermediary security services, clarifying the permissible outsourcing scope. Collectively, the US possesses high-profile advantages in resources, design, and implementation, indicating that the country is well-equipped to carry out stringent governance over PSCs, contingent on sufficient political will.

5.1.2. Weak Governance Willingness

Despite strong governance capacity, the US exhibits persistently limited governance willingness rooted in three interrelated factors: prevailing normative frameworks, strategic culture, and institutional frictions. First, the US has long adhered to a liberal ideology that privileges market rationality over state intervention. The privatization of security functionality is viewed not as an aberration but as an instrument for improving governance efficiency, conserving public resources, and externalizing political risks. Second, strategic preferences for global military deployment further dilute governance willingness. Compared to conventional armed forces, PSCs provide flexibility in managing complex and fluid geostrategic environments, executing policies of limited intervention, indirect projection, and unilateral engagement—while minimizing domestic political costs and scrutiny (Isenberg 2009). Finally, institutional frictions constrain governance willingness. Jurisdictional fragmentation

between federal and state governments, and among executive agencies and Congress, delays policymaking. Intensifying partisan polarization further obstructs legislative progress concerning PSCs' governance. Overall, congruence between prevailing norms and functional utility of PSCs reinforces strategic incentives and institutional disincentives to exert strong governance. These dynamics have entrenched the US as a proponent of moderate governance within the governance landscape.

5.2. Strict Governance: China

Since the 21st century, China's exponential expansion of overseas interests has elevated global security governance as a core national security agenda. International PSCs now play a prominent role in safeguarding personnel mobility and infrastructure development. Although a late entrant, the Chinese PSC industry has experienced rapid growth alongside the country's diplomatic flagship—the Belt and Road Initiative (BRI) (Badawi 2024). Nonetheless, cross-border operations remain tightly controlled under a defensive-centric governance model, reflecting a paradigmatic combination of governance capacity and willingness.

5.2.1. Strong Governance Capacity

Strict regulation of international PSCs in China is grounded in its mature governance capacity. The unitary, centralized political structure ensures power succession and regime stability, avoiding the regulatory fragmentation typical of federal systems, providing a predictable policy environment for managing sensitive domains like transnational security. The "tiao-kuai" (条块) administrative system enables vertical and horizontal integration between central and local authorities (Liu, et al. 2022). Although China has not enacted dedicated legislation for international PSCs, it maintains a comprehensive administrative framework governing corporate entry, personnel qualifications, and service scope. This "regulation-first" approach establishes a robust institutional foundation for further cross-border PSC governance. At the enforcement level, China exercises precise control over risk-prone nodes, particularly through weapon control based on personal jurisdiction. Firearms are prohibited abroad unless explicitly authorized by the state (Xin 2020), extending Weber's principle of violence monopoly into the global realm. This curtails sovereignty disputes and accountability dilemmas in host countries while ensuring PSCs operate within a defensive mandate, preventing the evolution into quasi-military entities. Furthermore, the Ministry of Public Security led a qualification assessment—license approval—dynamic supervision closed loop regulatory system. This preemptive and process-driven oversight far exceeds the more lenient post hoc accountability seen in other states.

5.2.2. Strong Governance Willingness

The principle of non-intervention constitutes a pillar of Chinese foreign policy, emphasizing sovereign equality, mutual non-aggression, and non-interference, reflecting a persistent commitment to the notion of absolute sovereignty. China's stringent regulation of international PSCs reflects the fundamental tension between

its governance willingness and normative adherence to the principle. The core contradiction lies in the transboundary nature of PSCs, whose ambiguous security responsibilities challenge the boundaries of sovereignty. While China rejects Western narratives such as humanitarian intervention and responsibility to protect (Mattlin 2010). Yet, the overlapping claims of personal and territorial jurisdiction in PSC operations render them vulnerably interpretable as an assertion of de facto extraterritorial projection of state power. China has long relied on consular protection and cooperation with host governments to safeguard overseas interests, demonstrating respect for sovereignty and international law. However, even limited involvement of Chinese PSCs in local security infrastructure, particularly in Global South countries, could provoke suspicions of neo-colonialism and undermine China's image as a representative of the Global South—despite the relatively modest presence of its PSCs compared to Western or Russian counterparts (Nantulya 2020). Under this willingness, a governance orientation of "limited openness under strict constraints" has emerged, curtailing systematic state support for PSCs and placing China at a relative disadvantage in the global market. Commensurately, with the BRI-accelerated "Going Global" (走出去) strategy, a growing number of Chinese citizens and enterprises venture overseas, facing highly complex and risk-laden security environments (Arduino 2018). Traditional reliance on diplomatic channels has proven insufficient to meet the multifaceted and transregional security demands. In response, Chinese nationals and enterprises are turning to PSCs for more targeted security solutions. This shift signals not only a rising market-driven demand for overseas security but also a disruption of China's strict governance logic—revealing a tension in the configuration of the state's role within the security governance of its global interests.

Chinese stakeholders have adopted two key strategies targeting overseas interests: the first is the "agent model," wherein the Chinese government and private actors assist host states in building local security capacities. This indirect approach allows China to safeguard its interests by empowering partner governments. With Chinese support, Pakistan established a comprehensive force integrating police and military personnel to provide full-spectrum protection for the BRI's critical project—the China–Pakistan Economic Corridor (CPEC), including the deployment of four maritime patrol vessels transferred from China, to secure the waters around Gwadar Port, with missions carried out by the Pakistani Navy (Kumar 2024). The second strategy involves cultivating "alternative" international PSCs—entities majority-owned by Chinese capital but managed by international professionals. They are registered in third countries to circumvent domestic regulatory constraints, enhancing operational flexibility. A leading example is Frontier Services Group (FSG), headquartered in Hong Kong and led by Erik Prince, founder of Blackwater. As the first PSC funded by Chinese capital and operated by American professionals, including retired US military officers, FSG provides security services for Chinese private and state-owned enterprises (Arduino 2017), such as the China National Petroleum Corporation (CNPC), engaged in infrastructure and energy projects

across the Global South.

5.3. Absent Governance: Sierra Leone

During Sierra Leone's state transformation, international PSCs such as Sandline International and Executive Outcomes were involved in the civil war, with the latter directly engaging in combat. Although PSCs temporarily stabilized the conflict, they failed to address its structural root causes. Their operations were also marred by humanitarian violations, raising concerns over legitimacy and moral justification. Sierra Leone's experience reflects a distinctive pattern in the Global South: states with weak governance capacity but strong governance willingness. This dynamic underscores the institutional gaps and strategic dilemmas such states face in reconciling sovereign authority with security and risk management.

5.3.1. Weak Governance Capacity

Shaped by colonial rule, independence struggles, and civil conflict, Sierra Leone has gradually stabilized its political landscape. However, its governance capacity remains weak, particularly in asserting nationwide administrative control and monopolizing the legitimate use of force. During the colonial era, the metropole adopted a low-cost governance strategy, concentrating institutional resources in urban centers while neglecting rural areas—entrenching a bifurcated urban–rural governance structure that persisted post-independence (Chakunda 2023). The reality of weakness was exacerbated by Cold War geopolitics, during which Western and Eastern blocs conferred de jure sovereignty to numerous African states, irrespective of their de facto governance capacities. At the same time, the postcolonial government's efforts to expand authority were hampered by a chronic shortage of institutional design and administrative resources. Consequently, many states retained international legal sovereignty without exercising meaningful domestic authority (Herbst 1997), subverting the state's monopoly on violence. Prolonged fragility and post-war residuals—such as blurred civil-military boundaries and the proliferation of small arms—created a vicious cycle. Non-state actors, local communities, and ethnic groups increasingly encroached on the state's coercive domain, fueling localized armed conflict. In this environment, Sierra Leone relied on asymmetrical partnerships with international PSCs, the bilateral dependency undermining its momentum rebuilding formal military and law enforcement systems—a pathological symptom of deeper governance failure. In many Global South countries, governance failure is compounded by political elites leveraging the government to outmaneuver rivals, converting the state into "comprador regimes" serving foreign interests, subordinating the welfare of their own citizens (Ndlovu-Gatsheni 2007). International PSCs frequently function as intermediaries between domestic and international stakeholders. Among these, Sierra Leone stands as a paradigmatic example of the overall phenomenon.

The Sierra Leone Civil War began in 1991. By 1995, the Revolutionary United Front (RUF) had gained a decisive advantage over government forces. In response, the government contracted the South African-based PSC Executive Outcomes (EO), which specializes in peacekeeping operations (Hough 2007). Within two

years, EO reversed the tide, expelled the RUF from Freetown, and stabilized key mining regions hosting the world's richest diamond fields. This compelled the RUF to enter negotiations, resulting in a 1996 peace agreement that paved the way for democratic elections. However, the peace process quickly collapsed when the RUF demanded the withdrawal of all foreign military personnel, leading to EO's contract termination in January 1997. Four months later, a military coup ousted the elected government, plunging the country back into war (Maciąg 2019). Despite EO's success, the backstage beneficiaries were not the Sierra Leonean people but foreign mining corporations, illustrating how security and stability were instrumentalized as bargaining tools for foreign investment. The EO-Sierra Leone collaboration exemplifies the portrayal of "resource curse" (Atkinson and Hamilton 2003) wherein external actors vying for strategic natural resources become a catalyst of economic stagnation and political instability, rather than development.

5.3.2. Strong Governance Willingness

Derived from anti-colonial memory, contemporary African states remain highly sensitive to external interference—a defining sentiment of their political culture. Nonetheless, former colonial powers have deployed mechanisms to impede full independence, notably using mercenaries as strategic instruments to reassert influence. Political instability enabled these actors to infiltrate domestic arenas, undermining sovereignty and weakening governance in nascent states. After the Cold War, international PSCs supplanted mercenaries, embedding themselves in complex relationships with local regimes and resource-based stakeholders, exacerbating governance deficits. Despite entrenched path dependency and a pronounced gap in governance capacity, the Sierra Leonean government demonstrated a notable willingness to regulate the operations of international PSCs.

The Global South's broader stance toward PSCs is reflected in regional institutional responses. African states were early adopters of regional instruments such as the Organization of African Unity (OAU) Refugee Convention and the Luanda Draft Convention, aiming to define and penalize mercenary-related human rights violations (Adamo 2020). These initiatives also contributed to the legislative development of Protocol I of the Geneva Conventions. The governance logic, denying legitimacy to private violent actors and imposing normative constraints, reflects a consistent caution toward PSCs in the Global South. In the 21st century, Sierra Leone launched systemic measures to evaluate the dual impact of PSCs on national security and public governance. The National Security and Central Intelligence Act delineated the respective mandates of private security actors, while the Office of National Security (ONS) was established as a dedicated agency tasked with supervising international PSCs (Abrahamsen and Williams 2005). Despite the existing regulatory loopholes and weak enforcement, the government proceeded a step to introduce the Standard Operating Procedures Manual for Private Security Companies (SOP), clarifying the scope of the Act and providing practical guidance for implementation, demonstrating an incremental yet deliberate effort to

institutionalize governance mechanisms (Abrahamsen and Williams 2009).

6. Implication and Conclusion

By analyzing international PSCs governance practices in the United States, China, and the Global South countries, this article develops and verifies a framework focused on governance capacity and willingness. The cross-case analysis reveals that these factors shape governance typologies and state roles vis-à-vis non-state security actors, contributing to a more systematic understanding of strategic divergence and institutional evolution governing international PSCs.

As PSCs expand their roles in global conflict zones and high-risk regions, they have evolved beyond auxiliary support to state apparatuses, forming transnational security supply networks. This shift exacerbates regulatory ambiguities and misalignments of authority, particularly in the Global South, where fragile institutions struggle to manage associated human rights and legal risks. Unilateral governance structures are no longer sufficient. Instead, a multi-level, inclusive architecture is needed. At the global level, binding international conventions should be pursued, building upon existing soft law instruments. For Global South countries with limited governance capacities, regional mechanisms under the auspices of intergovernmental organizations can reflect spatial particularities and consanguineous security demands. Nationally, states must integrate domestic regulatory development, resource allocation, and interdepartmental coordination to ensure policy coherence and operational viability, while mechanisms for information disclosure are essential to building public trust. Equally important is fostering normative resonance, as governance willingness is shaped by how international norms are interpreted and internalized within specific political and cultural contexts. For instance, while the US promotes institutional export and outcome-based governance, its overreliance on PSCs has eroded legitimacy and led to regulatory inconsistencies and governance loopholes. Conversely, although upholding the non-interventionist doctrine, China has pragmatically recalibrated its posture to accommodate growing overseas interests, highlighting that norm internalization is a dynamic, strategic process.

As an exploratory study, this article identifies several avenues for future research. First, a dynamic theoretical lens could better capture how national governance strategies adapt to geopolitical and geoeconomic shifts, regime transitions, or external security pressures—addressing the limitations of static typologies. Second, for analytical clarity, the article consolidates "private military companies" and "private security companies" under the umbrella of international PSCs, excluding mercenaries. While this facilitates conceptual coherence, it may obscure legal distinctions and governance heterogeneity among consimilar actors. Third, governance capacity and governance willingness are treated as independent variables herein; their interactive effects—potentially reinforcing or constraining each other—warrant further investigation through quantitative modeling and causal path analysis. In conclusion, international PSCs have become pivotal non-state actors in

global security governance, raising not only technical and institutional challenges but also ideological and normative tensions around sovereignty reconfiguration and governance legitimacy. Only through the synergistic governance involving institutional collaboration, balanced resource allocation, and the cultivation of normative resonance can a holistic security governance regime be established that is legitimate, equitable, and sustainable.

References

Abrahamsen, Rita and Michael Williams. 2005. "The Globalisation of Private Security: Country Report: Sierra Leone." University of Wales, Aberystwyth.

___. 2009. "Security Beyond the State: Global Security Assemblages in International Politics." *International Political Sociology* 3(1): 1-17. https://doi.org/10.1111/j.1749-5687.2008.00060.x.

Acharya, Amitav. 2004. "How Ideas Spread: Whose Norms Matter? Norm Localization and Institutional Change in Asian Regionalism." *International Organization* 58(2): 239-275. https://doi.org/10.1017/S0020818304582024.

Adamo, Antonino. 2020. "Mercenaries or Peacekeepers? Comparing Executive Outcomes and ECOMOG in Sierra Leone." *Africana studia: revista internacional de estudos africanus* 33: 153-169.

Anyanwu, David. 2012. "The State of Private Security Companies in Trinidad and Tobago: Towards the Development of a Governance System." *African Journal of Criminology and Justice Studies* 6(1): 45-66.

Arduino, Alessandro. 2017. "China's Belt and Road Initiative Security Needs: The Evolution of Chinese Private Security Companies." *RSIS Working Paper* No. 36.

___. 2018. *China's Private Army: Protecting the New Silk Road*. Palgrave Pivot.

Atkinson, Giles and Kirk Hamilton. 2003. "Savings, Growth and the Resource Curse Hypothesis." *World Development* 31(11): 1793-1807. https://doi.org/10.1016/j.worlddev.2003.05.001.

Badawi, Habib. 2024. "The Dragon's Overwatch: Chinese Private Security Expansion in Latin America and the Caribbean." *Bulletin of "Carol I" National Defence University* 13(3): 7-26. https://doi.org/10.53477/2284-9378-24-27.

Bali, Sabeena, Line Barabant, Upasana Garoo, Elina Hammarström, Samuel Küng and Cristina Valdés Argüelles. 2024. *Governance of Private Security in the South Asia Region*. Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Baum, Joel, and Anita M. McGahan. 2009. "Outsourcing War: The Evolution of the Private Military Industry after the Cold War." *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.1496498.

Beyani, Chaloka, and Damian Lilly. 2001. *Regulating Private Military Companies: Options for the UK Government*. London: International Alert.

Boddi, Emmylou, Anna Marie Burdzy and Nelleke Van Amstel. 2016. *Putting Private Security Regulation into Practice: Sharing Good Practices on Procurement and Contracting*

2015–2016. Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Buckland, Benjamin S., and Anna Marie Burdzy. 2015. *Progress and Opportunities: Challenges and Recommendations for Montreux Document Participants*. Geneva Centre for the Democratic Control of Armed Forces (DCAF).

Button, Mark. 2007. "Assessing the Regulation of Private Security across Europe." *European Journal of Criminology* 4(1): 109-128. https://doi.org/10.1177/1477370807071733.

Chakunda, Vincent. 2023. "Rural and Urban Governance in Africa: The Case of Zimbabwe." In *Handbook of Public Management in Africa*, edited by Gerrit van der Waldt. Edward Elgar Publishing.

Checkel, Jeffrey T. 1999. "Norms, Institutions, and National Identity in Contemporary Europe." *International Studies Quarterly* 43(1): 83-114. https://doi.org/10.1111/0020-8833.00112.

Chen, David H. 2009. "Holding "Hired Guns" Accountable: The Legal Status of Private Security Contractors in Iraq." *Boston College International & Comparative Law Review* 32(1): 101-113.

Clanahan, Keric D. 2013. "Wielding a 'Very Long, People-Intensive Spear': Inherently Governmental Functions and the Role of Contractors in U.S. Department of Defense Unmanned Aircraft Systems Missions." *Air Force Law Review* 70.

Cockayne, James, and Emily Speers Mears. 2009. "Private Military and Security Companies: A Framework for Regulation." International Peace Institute. https://www.ipinst.org/wp-content/uploads/publications/pmsc_epub.pdf.

DeWinter-Schmitt, Rebecca. 2017. "International Soft Law Initiatives: The Opportunities and Limitations of the Montreux Document, ICoC, and Security Operations Management System Standards." In *Public International Law and Human Rights Violations by Private Military and Security Companies*, edited by Helena Torroja. Springer Cham.

Drew, Phillip, and Rob Mclaughlin. 2016. *Handbook the Use of Force by Private Security Companies*. Oceans Beyond Piracy.

Elsea, Jennifer K. 2010. *Private Security Contractors in Iraq and Afghanistan: Legal Issues*. Congressional Research Service.

Geneva Centre for the Democratic Control of Armed Forces (DCAF). 2016. *Legislative Guidance Tool for States to Regulate Private Military and Security Companies*. https://www.dcaf.ch/sites/default/files/publications/documents/Legislative-Guidance-Tool-EN_1.pdf.

Gwatiwa, Tshepo T. 2016. "Private Military and Security Companies Policy in Africa: Regional Policy Stasis as Agency in International Politics." *Scientia Militaria: South African Journal of Military Studies* 44(2): 68–86. https://doi.org/10.5787/44-2-1176.

Hammes, T. X. 2010. "Private Contractors in Conflict Zones: The Good, the Bad, and the Strategic Impact." *Strategic Forums* 60: 26-37.

Herbst, Jeffrey. 1997. "Responding to State Failure in Africa." *International Security* 21(3): 120-144. https://doi.org/10.2307/2539275.

Holmqvist, Caroline. 2005. "Private Security Companies: The Case for Regulation."

Stockholm International Peace Research Institute (SIPRI) Policy Paper No. 9.

Hough, Leslie. 2007. "A Study of Peacekeeping, Peace Enforcement and Private Military Companies in Sierra Leone." *African Security Review* 16(4): 7-21. https://doi.org/10.1080/10246029.2007.9627441.

Isenberg, David. 2009. "Private Military Contractors and U.S. Grand Strategy." *PRIO Report* 1. International Peace Research Institute, Oslo (PRIO).

Jefferies, Ian D. 2002. "Private Military Companies–A Positive Role to Play in Today's International System." *Connections* 1(4): 103–125. http://dx.doi.org/10.11610/Connections.01.4.08.

Joachim, Jutta, and Andrea Schneiker. 2012. "New Humanitarians? Frame Appropriation through Private Military and Security Companies." *Millennium: Journal of International Studies* 40(2): 365–388. https://doi.org/10.1177/0305829811425890.

Krahmann, Elke. 2005. "Private Military Services in the UK and Germany: Between Partnership and Regulation." *European Security* 14(2): 277–295. https://doi.org/10.1080/09662830500336185.

___. 2012. "From 'Mercenaries' to 'Private Security Contractors': The (Re)Construction of Armed Security Providers in International Legal Discourses." *Millennium: Journal of International Studies* 40(2):343-363. https://doi.org/10.1177/0305829811426673.

Kruck, Andreas. 2020. "Governing Private Security Companies: Politics, Dependence, and Control." In *The Governor's Dilemma: Indirect Governance Beyond Principals and Agents*, edited by Kenneth W. Abbott, Bernhard Zangl, Duncan Snidal and Philipp Genschel. Oxford: Oxford University Press.

Kumar, Devendra. 2024. "Securitisation of Economic Projects: A Case of Chinese Private Security Companies (PSCs) in Pakistan." *Journal of Defence Studies* 18(1): 104-130.

Liu, Wei, Toby S. James and Caixia Man. 2022. "Governance and Public Administration in China." *Policy Studies* 43(3): 387-402. https://doi.org/10.1080/01442872.2022.2054091.

Maciąg, Mateusz. 2019. "Engagement of Executive Outcomes in Sierra Leone–Utility Assessment." *Security & Defence Quarterly* 27: 57-71. http://doi.org/10.35467/sdq/112110.

Makki, Sami, Sarah Meek, Abdel-Fatau Musah, Michael Crowley and Damian Lilly. 2001. "Private Military Companies and the Proliferation of Small Arms: Regulating the Actors." *Biting the Bullet Briefing* 10. International Alert and Saferworld. https://www.files.ethz.ch/isn/124854/Btb_brf10.pdf.

Mattlin, Mikael. 2010. "A Normative EU Policy towards China: Mission Impossible?" *Working Paper* 67. Finnish Institute of International Affairs. https://www.files.ethz.ch/isn/120928/UPI_Working_Paper_67_2010.pdf.

Mourão, Rachel R., and Danielle K. Brown. 2025. "When the Right Riots: How Ideology, Protest Tolerance, Authoritarianism and News Consumption Affect Perceptions of the US Capitol Insurrection." *Mass Communication and Society* 28(1): 201-225. https://doi.org/10.1080/15205436.2024.2384932.

Nalbandov, Robert. 2009. "Battle of Two Logics: Appropriateness and Consequentiality in Russian Interventions in Georgia." *Caucasian Review of International Affairs* 3(1):

20-36.

Nantulya, Paul. 2020. "Chinese Security Contractors in Africa." Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2020/10/chinese-security-contractors-in-africa?lang=en.

Ndlovu-Gatsheni, Sabelo J. 2007. "Weak States and the Growth of the Private Security Sector in Africa: Whither the African State?" In *Private Security in Africa: Manifestation, Challenges and Regulation*, edited by Sabelo Gumedze. South Africa: Institute for Security Studies.

Novotný, Vilém, Michel Perottino and Martin Polášek. 2016. "Political Parties and the Policy Agenda." In *Handbook of Public Policy Agenda Setting*, edited by Nikolaos Zahariadis. Edward Elgar Pub.

Ortiz, Carlos. 2010. *Private Armed Forces and Global Security: A Guide to the Issues*. Santa Barbara: Praeger.

Pereira, Ricardo, Ana Luquett, Rui Forte, and Mohammad Eslami. 2023. "Chinese Private Security Companies and the Limit of Coercion." *Small Wars & Insurgencies* 34(8): 1532-1557. https://doi.org/10.1080/09592318.2023.2256645.

Rookes, Stephen, and Walter Bruyère-Ostells. 2021. "Mercenaries in the Congo and Biafra, 1960-1970: Africa's Weapon of Choice?" *Small Wars & Insurgencies* 33(1–2): 112–129. https://doi.org/10.1080/09592318.2021.1957535.

Ryngaert, Cedric. 2008. "Litigating Abuses Committed by Private Military Companies." *European Journal of International Law* 19(5): 1035-1053. https://doi.org/10.1093/ejil/chn056.

Saner, Raymond, Amaka Uchegbu and Lichia Yiu. 2019. "Private Military and Security Companies: Legal and Political Ambiguities Impacting the Global Governance of Warfare in Public Arenas." *Asia Pacific Journal of Public Administration* 41(2): 63-71. https://doi.org/10.1080/23276665.2019.1622325.

Schreier, Fred, and Marina Caparini. 2005. "Privatising Security: Law, Practice and Governance of Private Military and Security Companies." *DCAF Occasional Paper* 6.

Singer, P.W. 2002. "Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security." *International Security* 26 (No. 3): 186-220. https://doi.org/10.1162/016228801753399763.

___. 2004. "War, Profits, and the Vacuum of Law: Privatized Military Firms and International Law." *Columbia Journal of Transnational Law* 42(2): 521-549.

Smith, Steve. 1991. "Mature Anarchy, Strong States and Security." *Arms Control* 12(2): 325-336. https://doi.org/10.1080/01440389108403958.

Stinnett, Nathaniel. 2005. "Regulating the Privatization of War: How to Stop Private Military Firms from Committing Human Rights Abuses." *Boston College International & Comparative Law Review* 28: 211-223.

Vaux, Tony, Chris Seiple, Greg Nakano and Koenraad Van Brabant. 2022. "Humanitarian Action and Private Security Companies." *International Alert*. https://www.international-alert.org/publications/humanitarian-action-and-private-security-companies/.

Weber, Max. 1964. *The Theory of Social and Economic Organization*. New York: Free Press.
Williamson, Oliver E. 1991. "Comparative Economic Organization: The Analysis of Discrete Structural Alternatives." *Administrative Science Quarterly* 36(2): 269-296. https://doi.org/10.2307/2393356.

Xin, Tian. 2020. "Private Security Companies: Emerging Protectors of China's Overseas Interests." *China Quarterly of International Strategic Studies* 6(2): 205-221. https://doi.org/10.1142/S2377740020500104.

FUNDING INFORMATION: No funding was availed.

CONFLICT OF INTEREST STATEMENT: None.

DECLARATION: No AI and AI-assisted technologies are used for this paper.

DATA AVAILABILITY STATEMENT: This study is qualitative, hence no quantitative data is utilized. All the qualitative data that is utilized for this paper are properly cited, accessible, and available.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Achilles' Heel of Hashd al-Shabi: Ambitions and Weaknesses of Asa'ib Ahl al-Haq

MAJ Filip BANÁŠ*
*Department of Political Science, Masaryk University, Brno, Czech Republic
e-mail: 499475@mail.muni.cz
https://orcid.org/0009-0006-3101-882X

Abstract

This article examines the Iraqi pro-Iran Shia militia group Asa'ib Ahl al-Haq (AAH), focusing on its growing assertiveness vis-à-vis its partner militias from the Hashd al-Shabi umbrella group. Through the lens of the 'Networks of Rebellion' theory by Paul Staniland, modified to the Iraqi Shia militias' context by Renad Mansour, the article shows specificities of AAH's ideological leaning vis-à-vis its partner militias. Among these are the combination of firm pro-Iran stance, typical for Hashd militias, combined with Iraqi nationalist roots, beginning with the seminars that AAH's leader Qais al-Khazali attended under the patronage of the founder of the modern Sadrist movement. Influenced by its roots and current lack of lucrative high-ranking positions within Hashd, AAH keeps conflicting with other pro-Iran militias, the whole organization failing to display the coherence of its maternal Iranian Revolutionary Guards, regardless of their mutual resemblance. The article concludes with implications these intra-Hashd quarrels present for Western policy makers, especially given the currently weakened Iranian position in the region compared to its increasingly tighter grip on Iraq.

Keywords:
Iraq; Shia; Militias; Hashd al-Shabi; Asa'ib Ahl al-Haq; Qais al-Khazali; Kata'ib Hezbollah; Badr Brigades.

Article info
Received: 10 July 2025; Revised: 18 August 2025; Accepted: 12 September 2025; Available online: 6 October 2025

Citation: Banáš, F. 2025. "Achilles' Heel of Hashd al-Shabi: Ambitions and Weaknesses of Asa'ib Ahl al-Haq" *Bulletin of "Carol I" National Defence University*, 14(3): 208-220. https://doi.org/10.53477/2284-9378-25-44

Asa'ib Ahl al-Haq (AAH) is a Shia militia operating in Iraq, where it is currently involved in domestic politics. In the past, the group also used to support the regime of the former Syrian dictator Bashar al-Assad, allegedly defending Shia holy sites (Heras 2014). AAH is and has always been an overtly pro-Iran group (Zorri, et al. 2020, 38). Its leader, Qais al-Khazali, admitted he had had personal ties with the late general of the foreign branch of the Iranian Revolutionary Guards Corps (IRGC-QF), Qassem Soleimani, during the interrogation after his arrest by Coalition forces in 2007 (Roggio 2018). Heras (2014) further corroborates AAH's ties with the IRGC-QF. However, for the following article as well as a coherent and effective US counter-policy towards pro-Iran factions in the country, it is important to note that AAH does not adhere to the Iranian rule of the religious experts' *wilayat al-faqih* (or Velayat-e Faqih in Farsi). In this regard, AAH differs from other important pro-Iranian Shia militias banded under the Popular Mobilization Forces (*Hashd al-Shabi*), most notably Badr Brigades or Kata'ib Hezbollah. AAH instead follows the belief that Ummah (Muslim community) holds the power (Zorri, et al. 2020, 30), which makes the group somewhat less eager to be pro-Iranian in the Iraqi Shia context.

This distinction was important in its early genesis and its distinction from other Iraqi Shia militias. These militias adhere either to wilayat al-faqih, forming the core of *Hashd*; to Grand Ayatollah Ali Sistani's quietist doctrine[1]; or to Shia cleric and populist politician Muqtada al-Sadr's Iraqi nationalist ideas (International Crisis Group 2018, 3–4). AAH's genesis occurred in the context of violent post-2003 Iraq and the shift in intra-state dynamics in favor of the Shia majority. Before its genesis, AAH members were part of the infamous Mahdi's Army (Jaish al-Mahdi or JAM), led by the cleric from a prominent Shia family, Muqtada al-Sadr. However, AAH soon split from the JAM, following their respective leaders' differing ideas on what it means to resist American forces as well as the acceptable amount of Iranian support (Zorri, et al. 2020, 41). While Sadr staunchly opposed deeper Iranian involvement and malign investment in Iraq, Khazali welcomed it (International Crisis Group 2018, 4). AAH, together with Badr Brigades and Kata'ib Hezbollah, have, over the years, become the primary instrument of growing Iranian influence in Iraq[2].

However, more recently, Hashd militias appear to hide behind the façade of law and order for Iraq and strict adherence to Iran certain friction points. In the past, Hashd militias have been compared to the Iranian Revolutionary Guards (IRGC) in the way they managed to capture the state by abusing the existing law practices within the state (see e.g., Smith and Knights 2025, 667–68 or Al-Aloosy 2023, 210). Smith and Knights (2025, 673–75) label the so-called phenomenon as 'lawfare', i.e. non-kinetic way of launching a hybrid insurgency against the state while existing within

[1] The idea that religious leaders shall stay away from politics, a view that generally poses no threat to Iraqi independence and integrity.

[2] For putting profound emphasis on these three Shia armed groups when describing Iranian influence, see for example chapter in the book 'Rebel Governance in the Middle East' concerned with malign influence of those particular militias on Iraqi stability and ability to govern (Al-Aloosy 2023).

the state with the aim of regime change from within. Employing lawfare, Hashd militias have been able to overcome several setbacks, among those the 2019 popular Tishreen protests against Hashd's corrupted practices, significant electoral losses from the 2021 parliamentary elections, or the fact that the competing Shia anti-Iran Sadrist trend managed to come out of these elections with the highest number of votes.

Considering the uncontested fortunes Hashd militias experienced in Iraq in recent years (2022-2025), it is even more surprising that at the end of June 2025, the head of the Supreme Judicial Court, Jassim Mohammed al-Amiri, resigned, allegedly for health reasons. The judge was seen as issuing biased rulings, favoring Hashd al-Shabi's political wings over other Iraqi political actors, adding to the long-standing controversy of the Iraqi Supreme Judicial Court being at the center of many crises and political turmoil (Abdul-Zahra 2025). Notably, Smith and Knights (2025) describe the judicial body in similar terms, arguing that over the years, it has been won over by Hashd militias, either by blackmailing or bribing several key judges. The subsequent phase, triggered by Sadr Shia anti-Iran political party's resignation from politics on the pretext of protesting Hashd's corrupted practices, thus unwilling to form a coalition with Hashd parties (Taib Menmy 2024), is described by the authors as 'bloodless coup' (Smith and Knights 2025, 671; 679). Pro-Iran forces specifically pointed at that time at Sadr's lower-class Shia followers, overflowing the International Green Zone in protest of Sadr's resignation, claiming Hashd and its less powerful allies defended law and security against anti-system forces (Smith and Knights 2025, 669; for more detailed ethnographic insight into the dynamics of 2022 violent clashes between Hashd forces and Sadrist protesters, see also Foltyn 2023).

The recent setback in the area key to exerting a grip on Iraq, the Supreme Judicial Court, thus poses a threat to this monopoly and somewhat relaxes the above-mentioned assumptions that Hashd is another IRGC[3]. In line with Fanar Haddad's analysis (2018), I argue that although it might seem so, the reality is much more complicated, as Hashd militias form a block from sometimes diverging entities which do not even uniformly adhere to the wilayat al-faqih ruling system and tend to have diverging tendencies (see e.g., Foltyn 2023, 22), unlike the much more coherent IRGC. Previously, the lack of grasp on pre-Hashd Iraqi Shia militias was obvious during the US capture of Khazali (2007-2010), who warned the interrogators about the Iranian nuclear program and mentioned petty conflicts within the radical Shia camp. The interrogators were nevertheless more interested in the momentarily tactical advantages Khazali would grant them on the ground and failed to pay attention to this retrospectively key intel (Roggio 2018).

[3] Although the main judge behind Supreme Court's politicization and recent more and more obvious shift towards Tehran, Faiq Zaidan (see e.g. Uysal 2023), remains in power, marking Jassim Mohammed al-Amiri's departure all but decisive regarding independent judiciary in Iraq.

To help turn the tide of deepening Iranian influence within Iraq, the following article presents rifts and frictions within the Hashd pro-Iran camp, namely between AAH and other essential militias such as Badr Brigades or Kata'ib Hezbollah. The argument builds on different ideological foundations of essential Hashd components, as AAH traces its origins towards lower Shia classes, similarly to the Sadrist trend. Essentially, then, AAH has historically clashed with the Sadrist trend over the role of Iran in Iraqi politics and to extend over their own financial interests (Al-Salhy 2022) rather than on what form the political system should take. The Sadrist roots, together with long-standing staunchly pro-Iran stance, make AAH the possible Achilles' heel of Hashd al-Shabi in case the US or allied forces were to project their interests non-kinetically against Hashd in Iraq. In the following chapters, the article presents the analysis of Asa'ib Ahl al-Haq, founded as an Iranian proxy, following up on its current rebranding into a relatively more independent, less eagerly pro-Iran actor. Subsequently, the cases of clashes over influence, both political and economic, with other Iranian affiliates are presented, providing the reader with a clear idea of precisely why Hashd fails to be another IRGC. The article concludes by suggesting the advances of non-kinetic policy against diverging Hashd components.

Genesis and Early History

In 2004, shortly after Muqtada al-Sadr's loosely controlled JAM was founded and started fighting the Coalition forces in Iraq, Khazali was banished from JAM. The conflict occurred over the alleged Khazali's refusal to follow orders from Sadr, whom he perceived as paranoid and incompetent. This was confirmed in the declassified interrogation of Khazali during his arrest in 2007-2010 (Zorri, et al. 2020, 41). Sadr has always had a complicated relationship with Iran and IRGC-QF, sometimes reluctantly accepting its patronage, other times furiously arguing against the Islamic Republic's involvement in Iraqi matters (O'Leary and Heras 2021, 50–52). The AAH leader Qais al-Khazali, on the other hand, never had any problem accepting Iranian patronage, which led to direct leadership from the IRGC-QF and Lebanese Hezbollah during the early days of the group's existence.

It is important to note here that the IRGC-QF applies against Iraqi Shia Militias what Zorri, Sadri and Ellis (2020, 10–11) describe as the 'Empower-Divide-Control' approach. It is a key principle in the successful effort of the IRGC-QF to penetrate radical Shia space in Iraq. Iranians usually start new or win over existing Shia militias; sow dissent among them or use existing frictions to split the group; and finally abuse the resulting power dilemma by offering weakened groups vast Iranian resources, while manipulating the installed second-tier leaders. Notably, not always must leaders be second-tier. In the case of several most prominent and, in the Iraqi society, most entrenched Shia militias, their leaders are or until recently were figures of profound importance, cooperating with Iran since the 1980s. Such figures are Hadi al-Amiri, leader of Badr Brigades, or the late leader of Kataib Hezbollah (KH), Abu Mahdi al-Muhandis. Nowadays, Qais al-Khazali belongs in this camp,

following Iran far too long to be simply discarded as another obedient servant. Zorri, Sadri and Ellis (2020, 37) even place AAH next to the Shia militias Badr Brigades and Sadrist Saraya al-Salama (Peace Brigades), each, at times, representing an important Iraqi Shia political party. The former used to represent the SCIRI/ISCI party (Supreme Council for the Islamic Revolution in Iraq/Islamic Supreme Council of Iraq) before launching its own political activities, whereas the latter represents the Sairoon coalition[4], specifically its Sadrist component. AAH, as the last piece of the puzzle, was used to fulfill armed tasks of the oldest Iraqi Shia political party, the Da'wa party, although AAH militarily represented the Da'wa party only unofficially, unlike the other prominent militias.

[4] Currently rebranded to 'Shiite National Movement', following yet another Sadr's retirement-return move between 2022 crisis and 2024 (Al-Jazeera 2024). It should be noted that Sadr's militias or political wings, although possessing different names at different times, are essentially still military and political segments of the Shia Iraqi nationalist movement around his person.

However, already in the 2014 Iraqi parliamentary elections, AAH founded its own political party, al-Sadiqun (the Honest Ones), running independently. Perhaps due to winning only 1/329 seats in the parliament, in the next elections (2018), al-Sadiqun joined the Fatah Alliance. This coalition has been, since its inception, composed of pro-Iranian winners over ISIS: political wings of groups such as Badr, KH, or AAH. The Fatah Alliance ended up second, with the Da'wa party ending up fifth with 25 seats and losing 67. This raises the question of where the AAH loyalty currently lies, since joining Fatah contributed to the Da'wa party's defeat in 2018. The truth might be more nuanced. Recent smirky AAH campaign against its political opponents, including old videotapes of its Shia rivals allegedly supporting the Ba'ath party, spared the Da'wa. However, only on the pretext of the Da'wa not crossing AAH's interests (Malik 2024). Later on, AAH and Da'wa joined voices to criticize AAH's fellow Hashd militia, Badr Brigades, marking the relationship between AAH and Da'wa at least pragmatically still alive (Al-Kaabi, et al. 2024).

Ideology and Constituency: Prerequisites for AAH-pivoted Intra-Hashd Conflicts

In the pre-ISIS and early ISIS period of Iraq (roughly 2011-2014), AAH participated in many purges in the Anbar and Diyala regions, as well as in Baghdad and southern Basra. The purges were conducted to suppress growing Sunni resentment towards what many perceived a sectarian-driven policies of then-Iraqi PM Nuri al-Maliki. The late PM even openly encouraged AAH members to join the Iraqi security apparatus, which he then used in his sectarian goals (Heras 2014). Notably, ISIS was able to spread so quickly through the Sunni parts of Iraq in no small part due to Maliki's politics, alienating all but Shia pro-Iranian Iraqis. Sunni Iraqis perceived ISIS as a lesser of two evils compared to the Iraqi security apparatus, in the beginning of the 2010s already firmly in the hands of Shia leaders advocating sectarian behavior (Zorri, et al. 2020, 50). AAH was one

of the heaviest Shia catalysts of sectarian violence[5]. For the involvement in numerous lethal suppressions of demonstrations and its use of violence against civilians, in 2019, the US Treasury Department imposed sanctions on al-Khazali and his brother, and in 2020, the US State Department designated AAH and both Khazalis as terrorists (Knights 2023).

By supporting the sectarian violence and creating a constant security dilemma, together with its strategy 'Divide-Empower-Control' described above, Iran heavily contributed to the ISIS resurgence and the subsequent need to create militias to protect Baghdad and conduct a counteroffensive. Its preference for a weak Iraq, divided over sectarian lines, is clear from the fact that the most prominent Iraqi Shia militias supported by Iran also contributed heavily to the poor security situation in the first place. Through militias such as AAH, Badr Brigades, or KH, Iran managed to entrench itself in Iraq even more, creating an aura of indispensability. It is believed that even a firm critic of Iranian (American, or any other) influence in the country, Muqtada al-Sadr, knows that Iraq in its current state cannot exist without Iran (O'Leary and Heras 2021, 70–71). With its overall weakness, militias such as AAH and others, pro-Iranian or not, are the alpha and omega of the current Iraqi ability to defend its territory. They effectively *are* the state.

However, AAH has a history of disobedience towards the Iraqi state and, recently, on certain occasions, towards their Iranian patrons as well (Knights 2023). This might suggest growing independent tendencies within the militia, perhaps following the Sadrist movement example, which also used to accept more Iranian patronage than it does nowadays. Furthermore, similarly to its group of JAM/Sadrists origin (and contrary to, for example, KH), AAH possesses a constituency of followers from the civil sphere, running social services and providing job opportunities[6]. This tendency is described as a 'parochial network', contrasting the 'vanguard network' with its vertical chain of command, a handful of elite fighters, and a weak social base, typical for the above-mentioned KH (Mansour 2021).

The idea of parochial-vanguard dichotomy in the Iraqi context comes from an influential Chatham House study (Mansour 2021), although the idea itself dates back a bit further. In the book 'Networks of Rebellion: Explaining Insurgent Cohesion and Collapse', Paul Staniland categorizes rebel groups into four types based on relative levels of vertical and horizontal control. The two types often used for the Iraqi context by experts such as Mansour, Michael Knights, and others are typical for dominantly possessing either vertical ('vanguard') or horizontal ('parochial') networks, not both (those would be 'integrated' networks, see Staniland 2014). Knights (2024, 4) emphasizes that Hashd groups should be understood as more or less freely moving on the parochial-vanguard scale, rather than rigidly performing

[5] Together with Badr Brigades, for example, which during the fight with ISIS overran the city of Fallujah and had summarily executed civilians for an alleged collaboration with ISIS (Steinberg 2017, 5–6).

[6] The services in question are linked to Lebanon Hezbollah-style modus operandi of military and civil sphere, with the latter 'providing social services, schools, and mosque refurbishment to Iraq's rural poor' (Zorri, et al. 2020, 41).

either network's tasks. Nevertheless, the idea behind the distinction remains, implicating certain strong and weak points of each Hashd group depending on the level of embeddedness in society on one hand and specialization regarding Iranian kinetic regional interests on the other. One such weak point is the constituency from which the 'parochial' network draws its legitimacy. Behind all the glamorous wealth and recent aggressive tendencies to grab power from other Hashd groups, AAH possesses an ideology blend of resistance rhetoric and reliance on Iraqi nationalism to the extent arguably not present within other pro-Iran Hashd powerhouses.

Inna Rudolf follows Mansour in his differentiation between 'parochial' AAH and 'vanguard' KH by suggesting that, nowadays, there are precisely these two main contenders over the future course of Iraqi Shia 'Axis of Resistance': KH and AAH. The former is the main avatar of Iranian influence in the country, spreading the Islamic Republic's influence and arguing for wilayat al-faqih within Iraq and Shia jihad abroad (Rudolf 2024, 15–20). The latter argues for an Iranian advisory role and help, but not for its control over internal Iraqi affairs, which is linked to the Khazali's role as a student of the founder of the Sadrist movement, Muqtada's father, Grand Ayatollah Muhammad Sadiq al-Sadr. He taught his disciples that wilayat al-faqih is a noble goal to follow, but only when conditions are met to avoid the resulting regime being over-occupied with its own survival rather than guiding its citizens (Ibid. 13). Sadr the elder's teachings thus lie somewhere between the full acceptance of Iranian wilayat al-faqih and Ali Sistani's quietism, mixing Shiism with Iraqi nationalism. Sadr the elder's teachings shaped his son Muqtada (O'Leary and Heras 2021, 2), but also his protégé Qais al-Khazali. This is not to say that Khazali conflicts with Iran, but he is becoming more overtly pro-Iraq, showing signs of growing independence, and was occasionally willing to criticize late IRGC-QF leader Ismail Ghani. Other times, AAH acted independently on Iran when it broke the ceasefire Islamic Republic ordered its affiliates, responding to the assassination of Soleimani and Muhandis in January 2020. AAH even accused KH, following the Iranian order, of succumbing to foreign influence (Rudolf 2024, 11-16)[7].

Naturally, this somewhat schizophrenic attitude, reaching to both Iraqi Shia nationalists as well as adherents to the Iranian wilayat al-faqih system, makes AAH unique in the camp of otherwise staunchly pro-Iran militias. Badr Brigades, operating in Diyala province and enriching itself from direct illicit economic cooperation with IRGC over Iraq-Iran borders (Al-Aloosy 2023, 207–8), or Kata'ib Hezbollah, formed to spearhead spec-ops in Iraq and abroad on behalf of the Hashd formation, are clear Iran-backed militias, benefiting to the highest possible extent from the Islamic Republic's patronage. Notably, both militias were even founded by the

[7] AAH has not been uniformly accepted as the least pro-Iran Hashd militia, which is the premise lying in the core of my argument. Aymenn Jawad Al-Tamimi in past explicitly linked AAH to Khomeinist wilayat al-faqih (Al-Tamimi 2014). I argue that rather than showing my (and by extension others') mistaken arguments, Tamimi reporting AAH's adherence to wilayat al-faqih is linked to both the inherent AAH's closeness to its Iranian patron, but also to the fact that Tamimi wrote the report in 2014. Given that tendency to independent behavior within AAH can be observed growing gradually over time, Tamimi's point corroborate rather than dispute my argument. Furthermore, already then Tamimi reported that AAH not only proclaimed its loyalty to IRGC-QF and by extension Tehran, but also utilized images of late Sadr the elder to boost the impact on its original constituency (Ibid. 2014). Such images can be regularly found on the internet, further supporting the claim that AAH draws inspiration and indeed legitimacy from late elder Sadr's teachings and constituency.

IRGC, either in the 1980s to fight against Saddam forces in the Iraq-Iran war (Badr), or as a small, well-trained special force within the broader movement of Hashd militias (KH). On the other hand, AAH's local origins might explain the following chain of differences with other militias and disobedience to Iran.

Growing AAH's Assertiveness, or Theater for Divergent Constituencies?

The failure to follow direct orders from Tehran at the beginning of 2020 or criticism of IRGC-QF late-leader Ghani are only a tip of the iceberg regarding AAH's divergence from other Iraqi militia adherents to Iran. Starting after Soleimani and Muhandis' departure by MQ-9 Reaper drone in January 2020 and subsequent loss of two individuals able to hold together quarreling Hashd personalities, it began pushing for more power. In a move aimed towards pushing its own candidate onto the position of the new speaker of the parliament, AAH did not shy from attacking other militias, using dubious old videotapes of competing candidates allegedly celebrating the Ba'ath party. It is noteworthy that the opposing candidate was, among others, supported by Badr Brigades, the oldest and one of the most prominent Hashd militias, and also the prime target of AAH's 2023 smirky campaign (Malik 2024). Verbal attacks from AAH directed towards Badr and its leader, Hadi al-Ameri, labeled 'traitors', continued at the beginning of 2024. So did AAH's encroachment on Badr's traditional stronghold in the Diyala governorate. Repercussions of Ameri's actions directed to sustain his influence included assassinations of several of his relatives, coinciding with political fallout between Badr and AAH (Al-Kaabi. et al. 2024). Discords between those two Hashd segments, in fact not unique for AAH vis-à-vis competing 'vanguard' forces but present between, for example, Badr and KH's Hashd chief of staff, Abu Fadak, during the 2022 post-election crisis, show the loose nature of intra-Hashd processes (Foltyn 2023, 22). As such, the umbrella organization fails to display the coherence and unanimous devotion to Iranian interests typical of the IRGC.

Yet, the biggest contenders are not AAH and Badr. These appear to be in line with Mansour's analysis of 'parochial' AAH and 'vanguard' KH. In 2023, verbal exchange between these two started with KH's downplay of AAH's jihadist credits regarding the latter's fight against US forces stationed in the country, followed by AAH blaming KH for 'endangering' the resistance movement by publicly revealing its members (MEMRI 2023). The statements can be interpreted as KH apparently disagreeing with AAH's participation in politics and with their manner of shifting responsibility to attacks onto shadow groups. These tensions are not a coincidence, as Malik suggests that AAH is attempting to rip Hashd al-Shabi from KH's influence and grant the status of Hashd leader to one of its members. For this goal, another dirty campaign was launched, this time using (or abusing) photos of current Hashd chairman Faleh al-Fayyad shaking hands with Sunni Anbar tribal leader, blamed by pro-Iran Shias for facilitating Islamic State's rise a decade ago (Al-Kaabi and Malik 2024).

To sum up this chapter, AAH is becoming more overt in their discords with fellow pro-Iran militants. The reason behind this behavior shift, however, is difficult to establish without proper empirical evidence. It could be that AAH is becoming more Iraqi-nationalist, as suggested above in this article, by its adherence to Ummah rather than wilayat al-faqih, based on Sadrist populist roots. However, the personal ambition of Qais al-Khazali and the simple greediness of its members, both elite and ordinary, cannot be due to article design, either confirmed or ruled out as the primary factor. Furthermore, the latter explanation is suggested by authors cited throughout this chapter, hinting at AAH's feeling of exclusion from inner Hashd circles and their attempts to push back against established actors such as Badr or KH. A similar point is made by Hudhaifa Ebrahim (2024), linking various Hashd leaders' (incl. Khazali's) current inactivity vis-à-vis the rest of the Axis of Resistance to the wealth Khazali, Amiri, and others managed to accumulate over the years. Profit from the current corrupted reality means abandonment of previous ideological zeal, which means more room to drive a wedge between Hashd components. To make this point clear, considering US interests in the region is the purpose of the final chapter.

Conclusion: Towards A More Stable Iraq

The simplified view of the Iraqi context regarding the differences within the Shia camp has cost the US a lot. Roggio (2018) argues that the US failed to take advantage of petty conflicts within the Shia camp while it still had a significant amount of 'boots on the ground', especially during the 2007-2010 surge. Currently, there is a difference between KH[8], firmly in the Iranian grip and under its control, operating through its 'vanguard network' as described by Mansour (2021); and AAH, operating increasingly independently, which could potentially cause US' misreading of the situation by blaming Iran for deeds of its militias it increasingly fails to control. Such deeds would be either violent or, more likely, seemingly peaceful, as AAH's ultimate ambition seems to remain increasingly institutionalized in the political process while grabbing more and more power at the expense of others. Understanding the situation as it is and following the shifting alliances within the Iraqi Shia camp is thus of profound importance to the US's ability to assess each violent – or indeed suspiciously peaceful – incident in the region correctly.

[8] Or groups formed from KH after its leader Muhandis died together with then-leader of IRGC-QF general Soleimani in January 2020 during the US drone assassination.

The argument advanced throughout this article emphasizes that, as a 'parochial' network, AAH is rendered more vulnerable to its constituency's attitude towards it, likely limiting its potency in acting on Iran's behalf, no matter the dire situation of ordinary lower-class Iraqi Shia. Such vulnerabilities are easily exploitable if one wishes to showcase AAH's and Khazali's hypocritical face to its constituents (for a showcase, see e.g. Malik and Knights 2025), possibly stripping the group of public approval

and shifting an increased amount of lower-class Iraqi Shia towards the Sadrist camp. It is important not to make the mistake of assuming that Sadrists, not least Muqtada himself, accept US presence in Iraq or that they would make any meaningful ally to US interests. However, as much as Sadrists oppose the US, they hold similar resentment towards Iran, essentially being the lesser evil for US interests compared to groups such as AAH. The policy proposal is linked to Mansour's (2021, 32) concluding remarks that, guided by a clear strategy offered by the vanguard-parochial distinction, the policy makers are being offered an option to calibrate their actions against each Hashd component accordingly, instead of trying to either surgically remove the component or co-opt it within the system.

In general, the US should use any weapon it can against the growing political power of Iran in Iraq and at the same time omit the counterterrorist, kinetic strategy wherever possible, favoring broader, politically oriented approaches. This is especially true as the kinetic way might be tempting given that other Iranian proxies in the region were recently weakened by precisely this 'iron fist' approach. However, the US burned itself in Iraq already once, and as Smith and Knights (2025), Al-Aloosy (2023, 204–9), or others[9] show, Hashd militias are embedded in the Iraqi system to such an extent that the two are difficult to distinguish. In case of kinetic operations, they would a) overcome existing differences and band together, which might perhaps apply even to otherwise anti-Hashd Sadr, and b) mobilize resources to such an extent that even Hezbollah was not able to.

[9] See e.g. the analysis of informal competing networks in Iraq by Maria Luisa Fantappie (2024).

In the current situation, by no small means due to the lessons learned from Hezbollah's and indeed Iranian loss to Israeli technological superiority, Hashd militias exercise restraint towards both US and Israeli forces (Cafiero 2025). In case of hasty airstrikes due to a misread situation, however, this could change, especially given the lack of control the government exerts over Hashd in similarly tense situations (for the comparison with the 2022 crisis, see e.g. Foltyn 2023, 17). In such a scenario, the victims would consist not only of Hashd leadership, but due to the sensitive context given previous Western engagement in Iraq, also US and Israeli PR, and, as always, Iraqi civilians. Non-kinetic approach and asymmetric, hybrid actions aimed against Hashd domestic legitimacy, utilizing existing rifts between quarrelling Hashd factions, instead of traditional 'smart bombs', is thus the US's biggest chance to reverse Iraq's current course. This is, however, a goal whose fulfillment would take time to accomplish, resembling Selin Uysal's long-term proposal of generational change favoring Western-groomed judges in the highest ranks of Iraqi courts instead of those overtly favoring Iranian interests (Uysal 2023).

Such solutions require careful calibration of the US's actions, but in a country where kinetic operations failed from the very beginning of the 'War on Terror', they should be deemed necessary. This is especially true as hints on possible Hashd disarmament following the fate of the Axis of resistance elsewhere in the region would not mean their actual disappearance, but rather formal incorporation of these malign actors into Iraqi structures, as suggested by an Iraqi politician close to Hashd political parties (Rasheed 2025). Since Hashd tentacles now reach deep into various Iraqi economic and security sectors (Al-Aloosy 2023, 204–9; Smith and Knights 2025), this would mean finalizing almost 25 years of Iran's attempts to capture its Arab neighbor and the final nail to the coffin of Iraqi independence.

References

Abdul-Zahra, Qassim. 2025. "Iraq's Top Court to Resume Work after President Retires amid Controversy." AP News, June 30. https://apnews.com/article/courts-iraq-judges-resignation-supreme-court-8e2d5dab95f468354db98873da32dfba.

Al-Aloosy, Massaab. 2023. "Ruling Without Responsibility: Badr Organisation, Asaʿib Ahl al-Haq, and Kataʿib Hezbollah After Defeating ISIS in Iraq." 2023. In *Rebel Governance in the Middle East*, by Massaab Al-Aloosy. Springer Nature Singapore. https://doi.org/10.1007/978-981-99-1335-0_7.

Al-Jazeera. 2024. "Al-Sadr's Return to Iraqi Politics: Implications and Ramifications." Al-Jazeera, May 6.

Al-Kaabi, Amir, Michael Knights, and Hamdi Malik. 2024. "Hadi Al-Ameri's Bad(r) Month." The Washington Institute for Near East Policy, February 21. https://www.washingtoninstitute.org/policy-analysis/hadi-al-ameris-badr-month.

Al-Kaabi, Amir, and Hamdi Malik. 2024. "Qais Al-Khazali Calls for Faleh al-Fayyad's Removal as PMF Chairman." The Washington Institute for Near East Policy, March 16. https://www.washingtoninstitute.org/policy-analysis/qais-al-khazali-calls-faleh-al-fayyads-removal-pmf-chairman.

Al-Salhy, Suadad. 2022. "Iraq: Sadrists Attack Rival Factions in Basra to Choke off Their Funds." Middle East Eye, October 4. https://www.middleeasteye.net/news/iraq-sadrists-basra-rival-factions-attack-choke-funds.

Al-Tamimi, Aymenn Jawad. 2014. "Iraq: Who Are Asa'ib Ahl al-Haq Islamists?" Islamist Gate, March 6. https://www.aymennjawad.org/14510/iraq-who-are-asaib-ahl-al-haq-islamists.

Cafiero, Giorgio. 2025. "Iraqi Militias Kept Quiet in the Israel-Iran War. Will It Last?" The New Arab, July 3. https://www.newarab.com/analysis/iraqi-militias-kept-quiet-israel-iran-war-will-it-last.

Ebrahim, Hudhaifa. 2024. "From Pro-Iran Militia Leaders to Big Business and Billionaires." The Medialine: Trusted Mideast News, August 23. https://themedialine.org/top-stories/from-pro-iran-militia-leaders-to-big-business-and-billionaires/.

Fantappie, Maria Luisa. 2024. "Politicians, Officers and Political Transition: The Case of Post 2003 Iraq." *Third World Quarterly* 45 (10): 1608–26. https://doi.org/10.1080/01436597.2023.2227109.

Foltyn, Simona. 2023. "Protectors of the State? The Popular Mobilisation Forces During the Post-Election Crisis." With the University Of Edinburgh. Preprint, University of Edinburgh, April 5. https://doi.org/10.7488/ERA/5193.

Haddad, Fanar. 2018. "Understanding Iraq's Hashd al-Sha'bi." The Century Foundation, March 5. https://tcf.org/content/report/understanding-iraqs-hashd-al-shabi/.

Heras, Nicholas. 2014. "Iraqi Shi'a Militia Asa'ib Ahl al-Haq Expands Operations to Syria." The Jamestown Foundation, May 15. https://jamestown.org/program/iraqi-shia-militia-asaib-ahl-al-haq-expands-operations-to-syria/.

International Crisis Group. 2018. "Iraq's Paramilitary Groups: The Challenge of Rebuilding a Functioning State." ISG, July 30. https://www.crisisgroup.org/middle-east-north-africa/gulf-and-arabian-peninsula/iraq/188-iraqs-paramilitary-groups-challenge-rebuilding-functioning-state.

Knights, Michael. 2023. "Profile: Asaib Ahl al-Haq." The Washington Institute for Near East Policy, April 27. https://www.washingtoninstitute.org/policy-analysis/profile-asaib-ahl-al-haq-0.

___. 2024. "Shia Jihadist State Capture in Iraq." The Washington Institute for Near East Policy, August 5. https://www.washingtoninstitute.org/pdf/view/18888/en.

Malik, Hamdi. 2024. "Asaib Ahl Al-Haq and Badr Fall Out Over Controlling the New Parliamentary Speaker." The Washington Institute for Near East Policy, January 29. https://www.washingtoninstitute.org/policy-analysis/asaib-ahl-al-haq-and-badr-fall-out-over-controlling-new-parliamentary-speaker.

Malik, Hamdi, and Michael Knights. 2025. "Qais Al-Khazali Tries, Fails to Tone Down Militant Bluster." The Washington Institute for Near East Policy, June 26. https://www.washingtoninstitute.org/policy-analysis/qais-al-khazali-tries-fails-tone-down-militant-bluster.

Mansour, Renad. 2021. *Networks of Power: The Popular Mobilization Forces and the State in Iraq*. With Royal Institute of International Affairs. Research Paper / Middle East and North Africa Programme. The Royal Institute of International Affairs.

MEMRI. 2023. "Dispute Among Iraqi Shi'ite Militias Over Their Role In Escalation Of Attacks Against U.S. Forces In Iraq And Syria." MEMRI: Jihad & Terrorism Threat Monitor, November 27. https://www.memri.org/jttm/dispute-among-iraqi-shi%E2%80%99ite-militias-over-their-role-escalation-attacks-against-us-forces-iraq.

O'Leary, Carole, and Nicholas A. Heras. 2021. *Muqtada al Sadr and Neo-Iraqi Nationalism: Implications and Opportunities*. JSOU Press.

Rasheed, Ahmed. 2025. "Exclusive: Iran-Backed Militias in Iraq Ready to Disarm to Avert Trump Wrath." Reuters, April 8. https://www.reuters.com/world/middle-east/iran-backed-militias-iraq-ready-disarm-avert-trump-wrath-2025-04-07/.

Roggio, Bill. 2018. "Iraqi Militant Qayis Khazali Warned Us About Iran. We Ignored Him." Washington Examiner, September 7. https://www.washingtonexaminer.com/magazine/2625523/iraqi-militant-qayis-khazali-warned-us-about-iran-we-ignored-him/.

Rudolf, Inna. 2024. "All the Mahdi's Men: Contextualising Nuances Within Iraq's Islamic Resistance." *Studies in Conflict & Terrorism*, September 8, 1–27. https://doi.org/10.1080/1057610x.2024.2398678.

Smith, Crispin, and Michael Knights. 2025. "How Iran Aligned Militias Seized Iraq: Irregular Warfare, Lawfare and Regime Change." *Small Wars & Insurgencies* 36 (4): 659–97. https://doi.org/10.1080/09592318.2025.2471644.

Staniland, Paul. 2014. *Networks of Rebellion: Explaining Insurgent Cohesion and Collapse*. Cornell Studies in Security Affairs. Cornell University Press.

Steinberg, Guido. 2017. "The Badr Organization: Iran's Most Important Instrument in Iraq." Stiftung Wissenschaft und Politik, July 21. https://www.swp-berlin.org/en/publication/the-badr-organization-irans-instrument-in-iraq/.

Taib Menmy, Dana. 2024. "Will Iraq's Muqtada al-Sadr End His Political Quarantine?" The New Arab, April 10. https://www.newarab.com/analysis/will-iraqs-muqtada-al-sadr-end-his-political-quarantine.

Uysal, Selin. 2023. "Making Sense of Iraq's Politicized Supreme Court Rulings." The Washington Institute for Near East Policy, December 4. https://www.washingtoninstitute.org/policy-analysis/making-sense-iraqs-politicized-supreme-court-rulings.

Zorri, Diane Maye, Houman A. Sadri, and David C. Ellis. 2020. *Iranian Proxy Groups in Iraq, Syria, and Yemen: A Principal-Agent Comparative Analysis*. JSOU Report 20–5. JSOU University Press.

Funding

The author reports there were no grants or additional funding for writing the manuscript.

Conflict of interest disclosure

The author reports there are no competing interests to declare.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Strategic Management of Emerging Technologies in NATO: A Framework for Foresight, Innovation, and Ethical Integration

Assistant Professor, Abdulkadir AKTURAN*
*Faculty of Economics and Administrative Sciences, Piri Reis University/Türkiye
e-mail: aakturan@pirireis.edu.tr
https://orcid.org/0009-0008-9107-0333

Abstract

The fast rise of artificial intelligence (AI), autonomous systems, and quantum technologies is changing the strategic context of national security. This paper examines how NATO countries can utilize new and Emerging Disruptive Technologies (EDTs) to enhance security and resilience across the Alliance. Using a multi-theoretical framework that combines dynamic capability theory, strategic foresight, military innovation, and technology governance, this discussion explores ways NATO could sense, seize upon, and transform itself in response to technological disruption. This article uses an exploratory qualitative design that combines policy and document analysis to examine institutional policy and lived stakeholder experiences related to technology integration and innovation management. The major issues emerging include variations in capacity for strategic foresight across member states that lead to bureaucratic inertia when some hold back others who want to move forward, put more fragmentation on already piecemeal interoperability standards, and add even more barriers because ethical normative differences are treated as if they belong elsewhere but weigh indeed. Defense Innovation Accelerator for the North Atlantic (DIANA) and the NATO Innovation Fund infrastructure notwithstanding, national procurement laws, security clearance regimes, and ethical misalignments limit their impacts. Responding to this analysis, therefore, requires proposing a strategic management approach under a four-pillar model that includes strategic foresight, organizational agility, capability integration, and ethical governance. A few of the recommendations are the establishment of a NATO-wide Joint Foresight and Technology Assessment Center, together with harmonization of dual-use procurement procedures, as well as the requirement for mandated national AI ethics frameworks in conformity with alliance-wide interoperability goals. These are steps toward making NATO adaptive and innovative under collective security postures while technological change is accelerated.

Keywords:
Strategic Management; Emerging and Disruptive Technologies; Ethical AI in Defense; Defense Innovation Accelerator; NATO; Military Innovation.

Article info
Received: 25 July 2025; Revised: 29 August 2025; Accepted: 10 September 2025; Available online: 6 October 2025

Citation: Akturan, A. 2025. "Strategic Management of Emerging Technologies in NATO: A Framework for Foresight, Innovation, and Ethical Integration." *Bulletin of "Carol I" National Defence University*, 14(3): 221-244. https://doi.org/10.53477/2284-9378-25-45

Introduction

Emerging and disruptive technologies, accelerating the proliferation of artificial intelligence, autonomous systems, and quantum computing, are changing the nature of modern defense alliances at the strategic level. For NATO, therefore, technological disruption becomes a case of critical opportunity mingled with urgent governance challenges. As military capabilities are reshaped, NATO will have to go beyond responding with changes in operational doctrines and relevant procurement mechanisms by instituting measures that would ensure agility, interoperability, and ethical coherence within its institutional setup. DIANA, the NATO Innovation Fund, and indeed even the Artificial Intelligence Strategy are all important tools recently added to its repertoire, but the innovation ecosystem remains fragmented. Variations at the national level in foresight capacities, procurement regimes, and ethical standards hamper allied efforts toward any collective response regarding rapid technological changes. Existing literature on military innovation and defense modernization primarily discusses either national systems or individual technology-related policies when, in fact, it is systemic and governance-level coordination that is missing within a multilateral institution like NATO. The study will therefore offer a strategic management view of how NATO could implement EDTs successfully across all its member nations, based on a multidimensional framework grounded in four interrelated pillars: strategic foresight, organizational agility, capability integration, ethics, and governance. The analysis is based on dynamic capabilities theory to assess institutional responsiveness; military innovation theory for providing a background to adaptation variability; anticipatory governance, and AI ethics frameworks through which normative issues can be problematized.

This paper uses an exploratory qualitative approach, combined with document analysis of NATO and national strategies, supplemented by examples of NATO member countries. These empirical findings are used to inform the development of a framework in guiding strategic responses to technological disruption.

Hence, this study tries to answer the following questions:

- How can NATO strengthen strategic foresight capabilities across member states to proactively adapt to emerging and disruptive technologies?
- What organizational and bureaucratic constraints hinder NATO's agility, and how can they be overcome to enable timely innovation adoption across the Alliance?
- What are the key technical and regulatory obstacles to achieving interoperability in emerging technology integration across NATO member states?
- How can NATO develop a unified ethical governance framework that reconciles diverse national approaches to AI and autonomous weapon systems?

It, therefore, falls within the strategic management and international security literatures that the paper contributes by offering, thus answering these very pertinent questions, some elements of implementable insights toward future-proofing policymakers for technological posture at NATO.

1. Theoretical Framework

This study applies a multi-theoretical lens in reviewing NATO's strategic management over emerging and disruptive technologies. The lens combines dynamic capabilities theory with strategic foresight, military innovation theory, and technology governance and ethics, thus allowing a comprehensive understanding of organizational, strategic, and normative dimensions regarding technological adaptation within the alliance.

1.1. Strategic Foresight

Strategic foresight is defined as the long-term technological development that could be anticipated within an institution and its potential impact evaluated for providing information for strategic decisions. In NATO's case, strategic foresight would assist in recognizing any new dangers or new possibilities arising and shaping technological priorities, determining where to make long-term investments in defense capability (Kupchyn, Dykhanovskyi and Kolotukhin 2020). A foresight-based approach to strategic foresight requires much more than keeping track of trends in technology; it includes scenario building, technology assessment, and strategic dialogue with stakeholders across the entire alliance. It is also significant to note here that NATO's Allied Command Transformation (ACT) does play a central role regarding strategic foresight; it needs coordination with National Foresight Units and different perspectives integrated towards enhancing the accuracy and relevance of future-looking activities (Nelson, et al. 2021). This paper discusses what changes can be made at the NATO level so that it will help strengthen strategic foresight capacity while anticipating newer technological challenges better.

1.2. Organizational Agility and Bureaucratic Constraints

Technological changes are supposed to be met with organizational agility. Bureaucratic processes, procurement systems, and multidimensional variations of national policies across the Alliance that lock timely innovation even when technological changes elsewhere in the world are embraced remain lodged (Herzog and Kunertova 2024; Shafiabady, et al. 2023). As advanced by the dynamic capabilities theory, this requires new strategic management inspired by a continuous process wherein an organization needs to develop abilities sequentially, sensing the opportunity, then seizing it through strategic action, followed by restructuring its internal structure accordingly (Teece 2007; Bitencourt, et al. 2020). For NATO, such necessary abilities are often limited because of fragmented governance and as a result of institutional inertia. According to dynamic capabilities theory, this means identifying opportunities and threats toward innovation and restructuring

the organization to maintain a competitive advantage under rapid changes in environments. For NATO, this theory helps analyze how it can adjust to technological shocks by carrying out environmental scanning and strategic investment activities, which are already being initiated through the Innovation Hub, DIANA, and the NATO Innovation Fund (Herzog and Kunertova 2024). These efforts mark what, in dynamic capabilities terms, is known as the ability of an organization to sense, seize, and transform dimensions of dynamic capabilities. Realizing such potential also requires parallel efforts in breaking bureaucratic barriers and agility enhancement among the member states (Bin 2018).

Institutional theory also considers the role of formal rules in channeling or constraining innovative behavior within large organizations (Scott 2013). Due to NATO's consensus decision-making and the sovereignty of member states, cross-border technological integration is often slowed down. To address such challenges, pathways for increasing flexibility modeled on agile governance, such as experimental procurement frameworks and public-private innovation hubs (e.g., Defense Innovation Unit (DIU), Cyber Innovation Hub (CIH)), could be pathways to further accelerate the adoption of emerging technologies (Rizzo, et al. 2020; Papanikolaou, et al. 2023).

1.3. Technology Integration and Interoperability Challenges

Military innovation theory thus becomes an appropriate approach to explain the uneven technological uptake among NATO member states by considering such key factors as threat perception, leadership orientation, organizational culture, and resource allocation toward new investments and operationalization of technologies (Filip 2022). These differentials within NATO result in different levels of technological readiness that create major problems for interoperability. Other countries whose infrastructure is not adequate and that have a parallel problem with bureaucratic inertia are falling behind the U.S. and U.K., which lead innovation due to strong infrastructure support plus an added dimension of more nimble private sectors involved in defense ecosystems (Horowitz and Pindyck 2022). Apart from widening this structural imbalance, which forms a barrier to overall technology integration, it further slows down the move toward standardization at the alliance level. Military innovation theory can help tease out ways in which these barriers could be lessened by working out how best to get more convergence and coordination across national systems that would drive interoperability for emerging technologies inside alliances.

1.4. Technology Governance and Ethics

Technology governance and ethics relate to normative management issues of dual-use and autonomous systems within disparate jurisdictions. It involves setting ethical considerations regarding the design and application of AI in warfare, ensuring accountability in applying autonomous weaponry, plus the risks correlated with new technological breakthroughs (Wyatt 2023). For NATO, technology governance and ethics acquire a special accent against the background of diversified legal and cultural

standards among member states because this is the very ground on which potential ethical disputes can destroy alliance cohesion (Roberson, et al. 2022). NATO faces the daunting task of creating shared ethical principles and governance frameworks that would respect national sovereignty on one hand, but ensure responsible innovation with new technology deployment, on the other (Danks and Trusilo 2022). This study explores how NATO can advance ethical technology governance as well as establish more general consent relating to matters of ethics in emerging technologies.

2. Methodology

This study utilizes a qualitative, document-based research design in probing the strategic management of emerging and disruptive technologies by NATO member states. The qualitative approach of this paper is justified since it endeavors to dwell much on the policy frameworks, institutional mechanisms, and normative dimensions that characterize such complexity in defense innovation and governance on an alliance-wide scale.

2.1. Document and Policy Analysis

The main sources of primary data for this research will be strategic documents, policy papers, and official statements publicly available from NATO and particular member states such as the United States, the United Kingdom, Germany, France, Poland, and Türkiye. Among others, key documents comprise:

- Emerging and Disruptive Technologies Roadmap for NATO.
- NATO Artificial Intelligence Strategy.
- National strategies on AI and defense innovation from the US, UK, and Germany.
- EU Strategic Compass plus appropriate publications of the NATO Innovation Fund.

The review of these documents was done in a systematic manner to extract themes, strategic priorities, and institutional challenges that have increasingly welcomed the adoption of emerging technologies and governance thereof. The selected documents were analyzed using thematic content analysis to extract key themes and insights relevant to NATO's technology strategy and governance. Themes were developed based on key areas of inquiry as established in the literature: strategic foresight, organizational agility, capability integration, and ethical governance. The analysis was manual but informed by a comparative reading across policy frameworks. The coding process was not software-assisted but rather interpretive, with iterative development of categories. It does not quantify frequency but seeks to draw meaningful insights regarding the institutional logic and strategic direction of NATO's technology management. This helps build a conceptual framework based on real-world policy discourse, ensuring academic inquiry as well as relevance to actual policy practice.

3. Findings and Analysis

This section presents an analysis of the findings from the policy and document analysis and expert interviews, focusing on key themes related to strategic management of emerging technologies, ethical considerations, and interoperability challenges within NATO.

3.1. Strategic Foresight across NATO States

Foresight is a strategic capability in leading the anticipation and preparation of possible technological upheavals and emergent threats (Durst, et al. 2014). An adequate level of foresight will enable the Alliance to surface potential opportunities and challenges it may face, inform its strategic decision process, and undertake pre-emptive resource allocation. However, disparities in capacity, coordination, and institutionalization characterize the current landscape of strategic foresight across NATO member states. Such imbalances impede the NATO effort from forming a cohesive, forward-looking approach to innovation in technology and uptake (Martins and Mawdsley 2021). Cyberspace became a crucial national security dimension recognized by NATO as a domain for collective defense, thus requiring military capability development (Bigelow 2019). Processes within Information Technology increase the precision of forecasts relating to any form of threat as well as mitigation so that weapons can be used against targets effectively under contemporary warfare scenarios (Naseem, et al. 2017). The use of Artificial Intelligence in the military has been growing recently and can influence both strategic and operational decision-making levels (Gaire 2023). Firms must invest in training in technical and soft skills to enable employees to maneuver successfully in the continuously changing landscape.

The greater interdependence of systems and reliance on data also enhances cyber risk; hence, robust measures and threat detection techniques should be instituted. Firms should adopt a proactive and future-oriented incident prevention approach, risk management approach, and real-time monitoring. Innovation requires psychologically safe workplaces, whereby employees feel free to share their thoughts with others- such a plan will ensure firms can shift when roles change as AI diffuses by providing learning opportunities for skill development. A cooperative grand cybersecurity strategy is thus required that enables an efficient political-military setup, besides a legal framework within which operational deliverables can take place (Efthymiopoulos 2019). Cooperation with NATO member states helps in resource sharing and specialized know-how through mutual defense arrangements (Reddy 2025). Modernization of European air forces improves defense capabilities for NATO with greater potential as more fifth-generation aircraft are added, decreasing the operational effectiveness of potential adversaries. Firms may also consider taking advantage of new opportunities to integrate cyber threat detection technologies, including AI threat detection and blockchain security technologies, which may assist in understanding evolving and generated cyber threats.

3.1.1. NATO's ACT Innovation Hub and Scenario Planning

The Allied Command Transformation Innovation Hub in Norfolk, Virginia, has been central to the support of long-range scenario planning for NATO (The Innovation Branch of NATO). The Innovation Hub conducts horizon scanning, technology assessments, and wargaming exercises as components in the sensitivity analysis concerning trend input and security environment disruptions. All these activities assist in building strategic insight capacity for long-term plans that NATO has to develop (Efthymiopoulos 2019). However valuable, this results in another problem for the ACT Innovation Hub: There is no coherent work with all national foresight units of NATO member states. This may allow parallel efforts to sprout in other places without drawing on the appropriate synergy and without a concerted approach to strategic foresight within the alliance. Strengthened by regular information sharing, joint workshops, and collaborative research projects, improved coordination mechanisms can make for heightened effectiveness and impact of NATO's foresight activities (Hanna, et al. 2017). NATO is dedicated to enhancing the readiness of its forces to address both present and future defense requirements, modernizing capabilities to safeguard all allies from any threat at any moment, and adopting a more comprehensive and synchronized approach to resilience (Mackenzie 2025). Consistent monitoring, security evaluations, and routine updates to security protocols are essential to sustain the operational resilience of the security framework and mitigate potential risks.

3.1.2. Variations in National Foresight Capacities

Major differences exist in the forecasting capacities of NATO member states. The U.K. and the U.S. Institutionalized forecasting capacity is quite established, with government agencies, research centers, and academic institutions specifically focused on strategic foresight and continuous technology assessment (Slapakova, et al. 2024). These are countries where horizon scanning, trend analysis, and scenario planning investments are made to inform defense and security policies. Some of the smaller NATO allies utilize such capabilities through outside vendors or the ACT Innovation Hub of NATO for strategic foresight activities. Such countries may not have resources, expertise, or even the institutional setup required to build such independent capability in forecasts (Németh, et al. 2018). This puts them in a situation where others external to their state carry out most of the functions and hence cannot root these functions into their specific national context and priorities. Differences in readiness and resilience presuppose variation in foresight capacities among all NATO member states. Some allies have an advantage in readiness to anticipate new threats and opportunities, while others lag behind (Németh, Dew and Augier 2018). Disparities such as these in the collective capacity of the alliance hinder it from responding effectively against multilayered security challenges. As an initial response to such a challenge, NATO may consider initiating capacity-building programs aimed at raising national foresight capabilities among less-resourced member countries (Pataki 2019). Such training could be technical assistance involving the actual funding of these countries in setting up foresight units as

well as strategies customized for technology assessment and long-term planning (Nelson, et al. 2021). Furthermore, fostering collaboration and knowledge sharing among NATO members can help bridge the foresight gap, ensuring that all allies benefit from emerging technologies and innovative approaches to security (Pataki 2019). Organizations would benefit from pursuing new opportunities to adopt cyber threat detection technologies, such as AI threat detection and blockchain security technologies, which may be of value for understanding evolving and generated cyber threats.

3.2. Organizational Agility and Bureaucratic Constraints

Organizational agility is the capacity to make adjustments in response to changes in situations, and for NATO to retain its technological advantage amidst technological disruption, it requires high organizational agility (Shafiabady, et al. 2023). Bureaucratic restraints and inflexible structures of organizations hold back an alliance from exercising its full potential in innovation and the right way of integrating new technologies, though (Herzog and Kunertova 2024).

3.2.1. DIANA Initiative and Cross-Border Innovation

One of the great steps towards agile cross-border innovation inside the alliance is the Defense Innovation Accelerator for the North Atlantic initiative (MITRE, 2024). DIANA will bind together innovative startups and technology companies with defense users throughout NATO member countries, offering important funding resources, expertise, and testing facilities (Mahnken 2018). It is this knowledge that DIANA seeks to bring to realization through accelerating cutting-edge technologies that can be applied to defense applications. Collaboration in developing advanced technologies does not guarantee success because of bureaucratic obstacles and regulatory hurdles that DIANA has to work its way around (Wilkinson and Jewell 2017).

The Defense Innovation Accelerator for the North Atlantic (DIANA) was launched in June 2023 as a flagship NATO project to provide support for dual-use technology innovation across the Alliance. It is headquartered in London with regional offices in Tallinn (Estonia) and Halifax (Canada), (Willows 2025). DIANA has 23 accelerator sites and 182 test centers throughout NATO member countries, supported by a value awareness with the NATO Innovation Fund (Collins 2024). DIANA assists startup and research teams exploring emergent technologies in fields such as quantum sensing, AI, autonomy, cyber resilience, and energy. Selected ventures go through a two-phase accelerator process. In the first phase, ventures can receive up to €100,000, and then up to €300,000 for phase two (Vincent 2024). Each phase also includes expert mentorship, access to NATO testing facilities, and opportunities to connect to investors. DIANA's activities align with the NATO Innovation Fund, which aids the development of strategic technologies.

Despite ambitious aspirations, DIANA faces institutional and regulatory challenges. Varied national procurement regulations almost invariably favor domestic providers

and inhibit cross-border participation, particularly for start-ups and SMEs. Moreover, differing security clearance processes across NATO members may limit timely access to test facilities and sensitive materials. These challenges hold back the mobility of talent and slow down the adoption of new technology. Nevertheless, DIANA has introduced practices that increase multinational cooperation and flexibility for procurement-like framework agreements and the Rapid Adoption Service. Therefore, DIANA is looking to establish an ecosystem for innovation that is structured and transparent to address legacy defense-industrial fragmentation and make NATO the leader in strategically significant technological innovation (National Defense Magazine 2025; DIANA RFP 2024). National procurement legislations tend to favor programs for newly established yet intently internalized defense contractors and restrict female participation as well as SMEs from other NATO nations (Ablazov and Radov 2020).

3.2.2. Public-Private Innovation Models

NATO may implement public-private innovation models that member states have already initiated. The CIH of Germany and the U.S. Defense Innovation Unit, for example, among others (Rizzo, et al. 2020), were meant to be initiatives through a partnership approach between government, industry, and academia towards development cooperation. Such organizations utilize flexible contractual arrangements, fast-tracked procurement processes, as well as methodologies based on agility for the swift realization of support systems in new technologies, assisting the deployment of innovative solutions. For instance, the CIH provides a program that gives funding access plus mentorship and market opportunities to cybersecurity startups and SMEs (Papanikolaou, et al. 2023). DIU works with commercial technology companies to develop and test prototype solutions addressing specific defense challenges. The private sector can deliver innovation acceleration capabilities that can significantly reduce time lags for capability realization. NATO needs to create collaborative ecosystems with the academic sector and the private sector for a wider reach of resources to build collaborative innovation. Collaborative ecosystems provide organizations with the opportunity to detect new combinations of innovation and leverage market opportunities while reducing risk (Schiuma and Carlucci 2018).

Recommendations

To enhance organizational agility and overcome bureaucratic constraints, NATO should consider the following recommendations:

Harmonize procurement laws and security clearance procedures: Member states should work to harmonize in tandem with NATO procurement regulations and security clearance processes. Barriers to cross-border innovation are reduced when harmonizing such regulations; therefore, more innovative startups and SMEs can participate.

Expand the use of flexible contracting mechanisms: NATO needs to use Other Transaction Authority agreements and more flexible contracting mechanisms, making the procurement process easier and allowing prototyping and experimentation to take place at the speed of relevance.

Foster a culture of experimentation and risk-taking: NATO should foster a culture of experimentation and risk-taking, encouraging defense organizations to embrace new technologies and innovative approaches to problem-solving.

These recommendations will build organizational agility in adopting technological advancements as well as speed up NATO's time to get involved with new technologies, and this will ensure that the alliance stays leading at innovation within the area of defense and security.

3.3. Technology Integration and Interoperability Challenges

A perennial challenge for NATO has been that of technology integration and interoperability due to sundry national systems, sundry levels of technological capacity, and sundry legal and ethical standards. Interoperability does not just mean some technical compatibility; it involves the readiness of systems, units, and forces to function harmoniously together in an integrated fashion.

3.3.1. Federated Mission Networking

NATO's Federated Mission Networking (FMN) architecture is the next big thing, or rather a progressive step in enhancing interoperability across member states (Hanna, et al. 2017). The move by FMN is geared towards coming up with a common technical framework for sharing information and collaboration within multinational operations. Providing standard protocols and interfaces, FMN intends to ease data and service exchanges between various national systems. However advanced FMN has made the world, real-time AI-based interoperability has taken a backseat across platforms, as Buřita et al. (2020) note. The integration of AI technologies into these systems will present new challenges in the field of interoperability due to different data formats, communication protocols, and security standards that will not allow them to efficiently exchange information and coordinate activities.

3.3.2. Alignment of Systems with Data and Legal Standards

Another challenge to the integration of technology into NATO is systems alignment with various data and legal standards (Mbah 2024). Different member states might use varying data formats, communication protocols, and security standards when developing their systems; therefore, it becomes very hard to exchange information and coordinate actions efficiently. Delays, mistakes, and vulnerabilities may be created in an uncoordinated multinational operation as a result of this misalignment. Some systems developed in the U.S., like Project Maven, which applies AI for intelligence analysis, may not immediately be compatible with European data protection regulations such as the General Data Protection Regulation (Schuett 2023).

Such mismatches delay the deployment of such systems within a multinational operation and will require expensive adjustments that will also take time to institute. The absence of common legal standards on the use of AI in military operations would rather open large gaps for legal uncertainty that can equally question NATO's actions' legitimacy and impair its effectiveness (Hill 2020).

Recommendations

NATO may want to prioritize increasing the interoperability of governance frameworks for AI and information-sharing systems within NATO itself and between it and non-NATO stakeholders (Kuziemski and Pałka 2019; Hanna, et al. 2017). Interoperability challenges are, therefore, not only matters for technical consideration but extend to ethics as well in view of the growing decisional autonomy of AI systems. Therefore, to help NATO address issues with technology integration and interoperability, it is recommended that NATO:

Establish Common Data Standards and Protocols: NATO would do well to design and urge the adoption of general data standards and communication protocols for AI systems as a way of ensuring that AI systems created by different member states can easily share information and coordinate activities, thus facilitating the flow of information between various national platforms.

Standardized Security Frameworks: NATO should standardize security frameworks and guidelines for AI systems, such that those systems meet the baseline level of security and resilience against any type of cyberattack or even a simple data breach.

Develop Mechanisms for Cross-Border Data Governance: NATO should put in place cross-border data governance mechanisms, making sure AI systems are in compliance with all relevant data protection regulations and standards of ethics (Mikhaylov, Esteve, and Campion 2018). Such mechanisms will enable secure as well as responsible sharing of information across all national borders while respecting individuals' right to privacy and keeping sensitive information secure (Sharma 2024). Standard protocols for secure information sharing, as well as legal frameworks, are also required by NATO that are compatible with the existing data protection regulations within member states; this means issues on data localization, retention, and access must be addressed so that AI systems can function optimally within diverse legal jurisdictions (Matthews 2022).

Promote the Development of Open-Source AI Platforms: NATO ought to be facilitating the advancement, development, and adoption of open-source artificial intelligence, as this will help enhance transparency and understanding of allied cooperation. This transparency would create the basis for ethical interoperability concerning AI systems if they conformed to the ethics we collectively accept and are accountable in the context of governance. This means NATO could solidify its strategic democratic

advantage and strengthen political unity across allied military forces (Danks and Trusilo 2022; Stanley-Lockman 2021).

Promote Joint Experimentation and Testing: NATO must encourage shared trial and error of AI systems in multinational setups, spotting and fixing interoperability issues early on. Dealing with these elements will set the stage for more integration and control steps at the AI–nuclear link (Chernavskikh 2024).
By solving these problems and using these tips, NATO can make it easier to add new technologies and ensure everything works well together with its many systems and tools. Also, NATO should bring back efforts for global rules and get ready for plans led by the United Nations to deal with stopped cyber fights (Taddeo and Floridi 2018).

3.4. Ethics and Governance

The ethical and governance dimensions of artificial intelligence and autonomous weapons systems are vital for NATO to consider, with respect to the likely implications for international security, human rights, and the laws of war (Roorda 2015). The discussions of autonomous weapons systems have raised sizeable legal and moral objections with respect to human control and whether there is a possibility of adhering to international law (Roorda 2015). Different views about the ethics of AI in warfare and the absence of regulatory instruments complicate matters for NATO. In my view, NATO needs to emphasize successfully developing ethical frameworks and governance regimes to ensure the responsible use of AI in defense applications that address ethical considerations throughout the life cycle of any technology from development to operational use (Taddeo, et al. 2021).

3.4.1. Divergent Ethical Approaches

Great divergence and difference of opinion are to be found within the NATO member states regarding the ethical frameworks governing Artificial Intelligence in military applications. Many of these perspectives flow from different national legal traditions, strategic priorities, and societal values. This makes for a complex challenge regarding the harmonization of policy across an alliance.

The United States often highlights AI as a means of gaining both strategic and operational advantages, which makes battlefield management better informed while reducing any time lag in decision-making, as well as ensuring the mitigation of risks to the friendly side, resulting in reduced casualties (Hagos and Rawat 2022). As articulated by Wasilow and Thorpe (2019), AI's capability can be leveraged to enhance situational awareness on the battlefield, speed up decision-making processes, and reduce risk to friendly forces, which consequently would reduce casualties during conflict. The practical benefits that artificial intelligence may provide relating to accuracy and swiftness, as well as effectiveness, are discussed, even regarding the necessity for in-situ learning of legal reviews concerning autonomous systems. This could be reflected in an increased appetite for discovery and subsequent usage of highly autonomous systems in precision targeting or complex logistics operations where the human is not directly involved.

Countries such as Germany and the Netherlands prefer a stricter policy, placing at the first plan of implementation strict adherence to international humanitarian law and fundamental human rights (Hill 2020). The core concern of this policy is to ensure that AI systems, particularly lethal ones, operate within existing legal and ethical frameworks and in meaningful human control in relation to all critical functions they undertake. These are the type of countries that lead advocacies for an international ban-or under very strict regulations on Lethal Autonomous Weapon Systems based on accountability principles and avoiding scenarios where machines may be allowed to make life-and-death decisions without proper human oversight. This ethical decision helps open wider societal debates regarding the morality of transferring such a substantial amount of decision-making authority to machines. Different ethical philosophies can influence national policies on the development and use of AI in military applications. This has become perhaps the most significant challenge to efforts at interoperability and a common strategic approach to AI across the Atlantic Alliance.

3.4.2. Absence of Harmonized Ethical and Regulatory Frameworks

The major challenge that NATO faces in the governance aspect of emerging technologies, especially in the case of autonomous weapon systems, is the absence of a universally binding ethical and regulatory framework. Scholars and experts have continuously identified this vacuum and reiterated the immediate necessity for an extensive, comprehensive set of rules to be developed by the entire alliance for ensuring responsibility in creating and using such systems (McFarland and Assaad 2023).

While the NATO Artificial Intelligence Advisory Board is in the process of efforts towards relevant policy guidance, member states have yet to share a common consensus on what level of human control over Autonomous Weapon Systems (AWS) is necessary and in what particular circumstances these systems can be effectuated both legally and ethically (McFarland and Assaad 2023). This highlights debates that are far from being resolved relating to conceptual and practical challenges toward an adequate prescription of "meaningful human control" within a technological environment increasingly dominated by levels of autonomy and intelligence. This has contributed to the development of a normative vacuum, one with the absence of explicit ethical prescriptions on one hand, and legally enforceable standards on the other. Such a vacuum does not inspire confidence in NATO's ability to control unintended consequences, whether those risks are related to escalation and miscalculation or breaches of international humanitarian law. Complicating matters is the fact that there are fundamental differences in ethical approaches between NATO member states. While some, led by the United States, give primacy to the pursuit of strategic and operational advantages, others, notably Germany and the Netherlands, emphasize international legal and humanitarian normative compliance (Hagos and Rawat 2022; Hill 2020; Wasilow and Thorpe 2019).

Only by bridging those normative differences will it be possible to develop some common ethical approach that would be seen as legitimate across the alliance.

Following the argument presented by Stanley-Lockman (2021), this should not be viewed primarily as a theoretical aspiration but rather forms an integral part of building trust and ensuring meaningful, real interoperability and moral credibility in ever-more-automated situations of conflict. It is here, therefore, that national AI ethics strategies need to match up with NATO's current drive for interoperability. Thus, support comes from Taddeo et al. (2021) in their call for harmonized ethical standards across member states to foster much-needed accountability, together with actual operational coherence and legitimacy in the new age of warfare driven by AI.

3.4.3. The Imperative for International Regulation and United Nations Initiatives

Considering the complications and consequences resulting from autonomous weapons, NATO should encourage and even reinstate efforts for international regulation led by the United Nations (Bode and Watts 2023). Another initiative that would require immediate action is preparing the ground for UN-led initiatives in stalled cyber conflicts, as well as ethical considerations of AI use in warfare; this is also essential for global norm and standard setting. The alliance can extend its hand in international dialogue cooperation by encouraging member states to participate actively in all relevant discussions within the UN concerning matters pertaining to autonomous weapons (Taddeo and Floridi 2018). Such collaboration with other nations and international organizations leads toward comprehensive regulation that is universal to cover the use of such technologies.

Recommendations

To address these ethical and governance challenges, NATO should consider the following recommendations (Matthews 2022):

Work on a unified ethical framework for AI in warfare: Shared values and principles are to lead NATO to the development of a unified ethical framework for AI in warfare. The major aspects that it should cover are human control, accountability, and transparency so that AIs can be used responsibly under existing international laws and with due respect to all ethical standards (Żurek, Kwik and Van Engers 2023). This includes rules for developing, deploying, and using AI-enabled weapons systems as well as means for monitoring and enforcing compliance.

Develop explicit legal norms for AWS: NATO ought to develop explicit legal norms for the design and utilization of autonomous arms, ensuring their compliance with war laws as well as ensuring that they do not pose unacceptable risks to civilians. This involves defining in detail what constitutes the scope of permissible uses, limitations on autonomy as well as safeguards against unintended consequences, and also under circumstances of escalation (Davison 2018). Explicit norms should respond to issues relating to target discrimination and proportionality, and the circumstances under which human intervention is required.

Dialogue and Cooperation on the Consideration of Ethical and Legal Issues: NATO should encourage international dialogue and cooperation on the consideration of ethical and legal issues regarding the use of AI in war with other international organizations and stakeholders, towards establishing common norms and standards. In this regard, NATO can also urge its member states to take a more active role in the relevant UN deliberations and negotiations concerning autonomous weapons (Taddeo and Blanchard 2023). By collaborating with other countries and international organizations, NATO will be assisting in the formulation of detailed codes jointly accepted internationally, controlling the employment of those technologies.

Tackling these ethics and governance challenges, as well as implementing these recommendations, will be important in how well NATO can use the advantages of AI and autonomous systems, meanwhile controlling their risks (McFarland and Assaad 2023). This requires an ongoing conversation that builds consensus between member states on ethical principles and clear ethical guidelines and legal standards reflecting shared values and principles, plus mechanisms to monitor compliance with rules and to address any unintended negative impacts resulting from deploying AI-enabled systems (Dodig-Crnković, Holstein and Pelliccione 2021).

4. Proposed Framework: A Strategic Management Approach

Successful integration and governance of new and emerging technologies in NATO requires a full strategic management framework involving strategic foresight, organizational agility, capability integration, and ethics & governance (Danks and Trusilo 2022). This is, in part, to assist NATO in responding dynamically to the challenges and opportunities offered by new technologies, while remaining true to its traditions, values, and principles (Pataki 2019). By taking a holistic approach to strategic management, NATO can help itself to exploit the opportunities of new technologies to increase its capability, strengthen its partners, and remain competitive in a fast-changing and increasingly complex security environment. Table 1 illustrates this framework:

4.1. Academic Underpinnings

The framework draws from well-known concepts in strategic management, innovation theory, and public policy. Strategic foresight falls within the general principles of anticipatory governance, whose main thrust is an advanced diagnosis of challenges and opportunities that may later be encountered (Khadri 2022). The notion of organizational agility corresponds to the prescription for flexibility and sensitivity in turbulent settings by organizational learning and changing management theory (Shafiabady, et al. 2023). Capability integration borrows from systems thinking and interoperability models, which stress harmonizing different elements

TABLE NO. 1

Strategic Management Framework for Emerging Technologies in NATO Member States

Dimension	Key Actions	Institutional Actors	Theoretical Basis
Strategic Foresight	Scenario planning and simulation exercises	NATO Allied Command Transformation	Anticipatory Governance
	Horizon scanning and technology trend analysis	Defense Advanced Research Projects Agency	Technology Forecasting
	Early warning systems for emerging threats	Defense Innovation Unit	Strategic Foresight methodologies
Organizational Agility	Agile procurement processes	Defense Innovation Accelerator for the North Atlantic	Agile Development methodologies
	Joint innovation accelerators and sandboxes	National defense ministries	Open Innovation
	Public-private partnerships for technology development	Venture capital firms and technology startups	Public-Private Partnerships
Capability Integration	Unified simulation platforms for joint training	NATO Consultation, Command and Control Agency (NC3A)	Systems Thinking
	Standardized data formats and communication protocols	National armed forces (e.g., U.S. Department of Defense)	Interoperability Standards
	Platform interoperability testing and certification	European Defence Agency	Joint Capabilities Integration and Development System
Ethics & Governance	Ethical review protocols for AI and autonomous systems	NATO's Data and Artificial Intelligence Review Board	Ethical AI principles (e.g., IEEE, Asilomar)
	AI governance frameworks and regulatory sandboxes	National AI ethics councils	Responsible Innovation
	Transparency and accountability mechanisms	International organizations (e.g., UN, EU)	Risk Management frameworks

toward the same end (Hill 2020; Porkoláb 2020). The ethics & governance leg sits in ethical canons for creating and using technology, plus modules on responsible innovation and risk management.

5. Discussion: NATO and the Challenge of Technological Disruption

NATO's successful technological engagement with emerging and disruptive technologies underscores the struggle between managing unity at the Alliance level and allowing space for member states' innovation freedom. Even though programs like DIANA and the NATO Innovation Fund were established to centralize and accelerate innovation (Kott, et al. 2018), different strategic prioritizations among member countries and various levels of technological competence across this Alliance continue to decentralize innovation practices (Zhang, Sun and Sun 2023). This situation brings about critical problems in terms of interoperability, standardization, and ethical governance, particularly when talking about artificial intelligence (AI) and autonomous systems' applications (Onderco 2025). The ability of NATO to predict technological disruption will also rely upon a strengthened mechanism in strategic foresight. There is currently no integrated foresight architecture that merges national-level anticipatory planning with the NATO-wide strategy. Though ACT and its Innovation Hub input by way of scenarios and trends, coordination with

national foresight units has not been on a consistent basis (Efthymiopoulos 2019). A "Joint Foresight and Technology Assessment Center" could provide comparisons of various national foresight perspectives for synthesis, which in turn would sustain collective strategic planning at the Alliance level to maintain long-term readiness. Where NATO's bureaucracy and different state acquisition processes slow down the timeliness of introducing innovations, organizational agility is equally critical apart from foresight (Herzog and Kunertova 2024). Large states are advantaged by infrastructure and an ecosystem of defense R&D; most small members do not have the human and financial capital to keep up. This creates problems with full participation that work against building momentum collectively (Akhmadi and Tsakalerou 2022; Jurak 2020). Therefore, there is a convincing need for NATO to standardize acquisition rules across its member states and also encourage the formation of joint procurement centers as well as implement experimental procurement forms, including innovation sandboxes and pilot initiatives that can be rapidly tested and afterward scaled up (Maagi and Mwakalobo 2023; Hasik 2024).

Another challenge that brings about other complications in this integration is interoperability. Military innovation theory is central to the explanation of differential rates of technological adoption across the Alliance, with a focus on national variations in threat perception, leadership, and institutional culture (Filip 2022). For example, innovation led by the U.S. and U.K. is followed by others, where bureaucratic inertia, among other shortcomings in infrastructure, happens to be a problem (Horowitz and Pindyck 2022). This creates disparities that later translate into harmonized AI architecture, data-sharing protocols, and cross-border capability integration. To crack these technical and regulatory hindrances, NATO needs advocacy through standardization for public-private investments in collaborative platforms that would forge ways for coordinated development and deployment of dual-use technologies. Perhaps even more formidable would be building common ground concerning an ethical and governance framework relating to AI and autonomous weaponry. The member states are as legally diverse in their ethical concerns related to issues of human control, responsibility, and data rights as the very technology itself complicates joint operations, makes the public lose confidence, and delays efforts at achieving interoperability systems (Aleksandra, et al. 2025; Holst, et al. 2024). In the absence of clearly defined roles and institutional mechanisms for oversight, it is difficult to assign responsibility when an accident takes place (Kandasamy 2024; Pham 2025). NATO should spearhead efforts at harmonization of national AI ethics policies and governance structures that would be transparent in matters relating to accountability as well as compliance with international norms. Cybersecurity has a place in the new order, too. Therein lies the requirements for an integrated cyber strategy encompassing AI-enabled threat detection, infrastructure protection through blockchain on one hand, and adaptive response mechanisms to digital resilience (Bondoc and Malawit 2020; Schiliro 2023; Shiny, et al. 2025). Public-private partnerships and closer collaboration with academic institutions will further support innovation while aligning technical

development with strategic needs (Efthymiopoulos 2019; Casady and Garvin 2022). NATO must simultaneously enhance its anticipatory capacities, remove bureaucratic bottlenecks, strengthen interoperability frameworks, and advance a shared ethical vision. Only by addressing these interconnected dimensions can the Alliance maintain its technological edge and strategic coherence in an era defined by rapid and disruptive innovation.

Conclusions

Emerging and disruptive technologies (EDTs) such as artificial intelligence, autonomous systems, and quantum computing grow ever more powerful at a dizzying pace, offering amazing opportunities yet posing daunting dangers for NATO. As proven by this study, managing these strategically within the Alliance calls for a multi-pronged plan that blends foresight with agility, capability integration with ethical governance. Analysis of results brings out into bold relief an urgently critical need for improved bureaucratic capacity at NATO as it tries to pole-vault above barriers in its current rules and regulations against the tide of technological disruption, on the one hand, to encourage interoperability while reconciling widely different ethical and legal standards among member states. The four-pillar framework, consisting of strategic foresight, organizational agility, capability integration, ethics, and governance, gives a holistic approach map through which NATO can find its way around the minefield of technological innovation. A NATO-wide Joint Foresight and Technology Assessment Center, accompanied by harmonized procurement procedures and mandated interoperable ethical frameworks for AI across the Alliance, would go far in bridging this innovation divide and enable collective responses to new forms of threats. Public-private partnerships, on the one hand, will be intensely fostered, and on the other hand, procurement streamlined to finally lead to market-leading technologies being dramatically more rapidly adopted; standardized data protocols and security frameworks themselves create enhanced interoperability.

At the heart of this strategic management approach lies ethical governance. Because ethical views differ between member states, NATO should adopt a consolidated framework that will equally weigh in the balance between providing an operational advantage and observing international humanitarian law as well as human rights laws. NATO has to spearhead the process of creating transparent and accountable as well as legally sound norms for the usage of autonomous systems so that technological advancement is in tandem with the spirit and letter of its founding principles and legal obligations. Ultimately, the achievement of enhanced fusion of EDTs into NATO's strategic posture depends on its adequate dynamism, inclusivity of cooperation, and responsibility in governance. It can do this by heeding the recommendations presented in this paper so as to future-proof its capabilities, reclaim the technological lead, and renew the collective security commitments against a backdrop of fast-paced change that is inherently unpredictable. The road

ahead calls for a commitment with equal value to ethical principles, innovation, and multilateral cooperation toward NATO being that resilient, adaptive agent amidst changing global challenges.

References

Akhmadi, S., and M. Tsakalerou. 2022. "Shades of innovation: is there an East-West cultural divide in the European Union?" *International Journal of Innovation Science* 15(2): 260-278. https://doi.org/10.1108/ijis-01-2022-0019

Aleksandra, N., J. Bojana, R. Maryan, and T. Dimitar. 2025. "Evaluating Trustworthiness in AI: Risks, Metrics, and Applications Across Industries." *Electronics* 14(13): 2717. https://doi.org/10.3390/electronics14132717

Bigelow, B. 2019. "What are military cyberspace operations other than war?." In *2019 11th International Conference on Cyber Conflict (CyCon)* (Vol. 900, pp. 1-17). IEEE. https://doi.org/10.23919/cycon.2019.8756835

Bin, A. 2018. "NATO's Defense Institution Building and Projecting Stability." *Connections* 17(3): 8-22. https://doi.org/10.11610/Connections.17.3.01

Binnendijk, A., G. Germanovich, B. McClintock and S. Heintz. 2020. *At the Vanguard: European Contributions to NATO's Future Combat Airpower* (No. RRA3111). https://doi.org/10.7249/rra311-1

Bitencourt, C.C., F. de Oliveira Santini, W.J. Ladeira, A.C. Santos, and E.K. Teixeira. 2020. "The extended dynamic capabilities model: A meta-analysis." *European Management Journal* 38(1): 108-120. https://doi.org/10.1016/j.emj.2019.04.007

Bode, I., and T.F.A. Watts. 2023. Loitering Munitions and Unpredictability. Autonomy in Weapon Systems and Challenges to Human Control. https://findresearcher.sdu.dk/ws/portalfiles/portal/231643063/Loitering_Munitions_Unpredictability_WEB.pdf

Bondoc, C.E., and T.G. Malawit. 2020. "Cybersecurity for higher education institutions: Adopting a regulatory framework." *Global Journal of Engineering and Technology Advances* 2(3): 016-021. https://doi.org/10.30574/gjeta.2020.2.3.0013

Buřita, L., J. Hrabovský, A. Novák, and P. Pohanka. 2020. "Systems Integration in Military Environment." *Advances in Military Technology* 15(1): 25-42. https://doi.org/10.3849/aimt.01334

Casady, C.B., and M.J. Garvin. 2022. "Progressive" Public-Private Partnerships: Are They Reformative or Regressive!?. *Public Works Management & Policy* 27(4): 342-346. https://doi.org/10.1177/1087724x221106164

Chernavskikh, V. 2024. "Nuclear weapons and artificial intelligence: Technological promises and practical realities." *SIPRI Background Paper*. https://doi.org/10.55163/vbqx6088

Collins, E. 2024. *NATO's DIANA Trans-Atlantic Network Expands With New Accelerator, Test Sites.* https://govconexec.com/2024/03/natos-innovation-network-adds-new-accelerator-test-sites/?utm_source=chatgpt.com

Danks, D., and D. Trusilo. 2022. "The challenge of ethical interoperability." *Digital Society* 1(2): 11. https://doi.org/10.1007/s44206-022-00014-2

Davison, N. 2018. "A legal perspective: Autonomous weapon systems under international humanitarian law." In Disarmament (p. 5). United Nations. https://doi.org/10.18356/29a571ba-en

Dewulf, A., and W. Elbers. 2018. "Power in and over cross-sector partnerships: Actor strategies for shaping collective decisions." *Administrative Sciences* 8(3): 43. https://doi.org/10.3390/admsci8030043

DIANA RFP. 2024. *Request for Proposal – Challenge and Accelerator Programme Implementation (NATODX-24-R-0005).* https://www.diana.nato.int/resources/site1/general/rfp%20-%20challenge%20and%20accelerator%20programme%20implementation%20-%20natodx-24-r-0005.pdf

Dodig-Crnkovic, G., T. Holstein, and P. Pelliccione. 2021. " Future intelligent autonomous robots, ethical by design. Learning from autonomous cars ethics." *arXiv preprint arXiv:2107.08122*. https://doi.org/10.48550/arxiv.2107.08122

Durst, C., M. Durst, T. Kolonko, A. Neef, and F. Greif. 2015. "A holistic approach to strategic foresight: A foresight support system for the German Federal Armed Forces." *Technological Forecasting and Social Change* 97: 91-104. https://doi.org/10.1016/j.techfore.2014.01.005

Efthymiopoulos, M.P. 2019. "A cyber-security framework for development, defense and innovation at NATO." *Journal of Innovation and Entrepreneurship* 8(1): 12. https://doi.org/10.1186/s13731-019-0105-z

Filip, S.O. 2022. *Critical success factors for European AI startups.* https://doi.org/10.13140/RG.2.2.19038.72006

Gaire, U.S. 2023. "Application of artificial intelligence in the military: An overview." *Unity Journal* 4(01): 161-174. https://doi.org/10.3126/unityj.v4i01.52237

Hagos, D.H., and D.B. Rawat. 2022. 'Recent advances in artificial intelligence and tactical autonomy: Current status, challenges, and perspectives." *Sensors* 22(24): 9916. https://doi.org/10.3390/s22249916

Hanna, M.W., D. Granzow, B. Bolte, and A. Alvarado. 2017. "NATO Intelligence and Information Sharing: Improving NATO Strategy for Stabilization and Reconstruction Operations." *Connections The Quarterly Journal* 16(4): 5. https://doi.org/10.11610/connections.16.4.01

Hasik, J. 2024. *Friend-sourcing military procurement: Technology acquisition as security cooperation.* https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/friend-sourcing-military-procurement/

Herzog, S., and D. Kunertova. 2024. "NATO and emerging technologies." *Naval War College Review* 77(2): 47-70. https://www.jstor.org/stable/48821934

Hill, S. 2020. "AI's Impact on Multilateral Military Cooperation: Experience from NATO." *AJIL Unbound* 114: 147-151. https://doi.org/10.1017/aju.2020.27

Holst, L., L. Lämmermann, V. Mayer, N. Urbach, and D. Wendt. 2024. *The Impact of the EU AI Act's Transparency Requirements on AI Innovation.* https://aisel.aisnet.org/wi2024/92

Horowitz, M.C., and S. Pindyck. 2022. "What is a military innovation and why it matters." *Journal of Strategic Studies* 46(1): 85. https://doi.org/10.1080/01402390.2022.2038572

Jurak, A.P. 2020. "The importance of high – Tech companies for EU economy – Overview and the EU grand strategies perspective." Research in Social Change 12(3): 32. https://doi.org/10.2478/rsc-2020-0013

Kandasamy, U.C. 2024. *Ethical Leadership in the Age of AI Challenges, Opportunities and Framework for Ethical Leadership.* arXiv (Cornell University). https://doi.org/10.48550/arxiv.2410.18095

Khadri, H.O. 2022. "Becoming future-proof STEM teachers for enhancing sustainable development: A proposed general framework for capacity-building programs in future studies." *Prospects* 52(3): 421-435. https://doi.org/10.1007/s11125-021-09588-0

Kott, A., P. Théron, M. Drašar, E. Dushku, B. LeBlanc, P. Losiewicz, ... and F. De Gaspari. 2018. "Autonomous intelligent cyber-defense agent (AICA) reference architecture. Release 2.0." *arXiv preprint arXiv:1803.10664.* https://doi.org/10.48550/arXiv.1803.10664

Kupchyn, A., V. Dykhanovskyi, and Y. Kolotukhin. 2020. "The war of the future as a strategic guideline for the forming the critical technologies list." *Social Development and Security* 10(1): 9-17. https://doi.org/10.33445/sds.2020.10.1.2

Kuziemski, M., and P. Palka. 2019. *AI governance post-GDPR: lessons learned and the road ahead.* https://doi.org/10.2870/470055

López, O.S. 2025. "Unlocking Regional Economic Growth: How Industry Sector and Mesoeconomic Determinants Influence Small Firm Scaling." *Economies* 13(5): 138. https://doi.org/10.3390/economies13050138

Maagi, B., and A. Mwakalobo. 2023. "Practitioners' Perception of the Effect of E-Procurement Practices on Time Saving in Public Procurement in Tanzania." *Open Access Library Journal* 10(5): 1-18. https://doi.org/10.4236/oalib.1110075

Mahnken, T.G. 2018. "Innovation in the interwar years." *SITC Research Briefs* (2018-11). https://escholarship.org/content/qt1hw200dw/qt1hw200dw.pdf?t=p9joni

Martins, B.O., and J. Mawdsley. 2021. "Sociotechnical imaginaries of EU defence: The past and the future in the European defence fund." *JCMS: Journal of common market studies* 59(6): 1458-1474. https://doi.org/10.1111/jcms.13197

Matthews, D. 2022. "UK rejects EU approach to artificial intelligence in favour of 'pro-innovation'policy." *Science Business*. https://sciencebusiness.net/news/uk-rejects-eu-approach-artificial-intelligence-favour-pro-innovation-policy

Mbah, G.O. 2024. "Data privacy in the era of AI: Navigating regulatory landscapes for global businesses." *Int. J. Sci. Res. Anal* 13(2): 2396-2405. https://doi.org/10.30574/ijsra.2024.13.2.2396

Mackenzie, H. 2025. "The North Atlantic Triangle and North Atlantic Treaty: A Canadian Perspective on the ABC Security Conversations of March-April 1948." *London journal of Canadian studies* 38(1): 65-92. https://doi.org/10.14324/111.444.ljcs.2025v38.006

McFarland, T., and Z. Assaad. 2023. "Legal reviews of in situ learning in autonomous weapons." *Ethics and Information Technology* 25(1): 9. https://doi.org/10.1007/s10676-023-09688-9

Mikhaylov, S.J., M. Esteve, and A. Campion. 2018. "Artificial intelligence for the public sector: opportunities and challenges of cross-sector collaboration." *Philosophical transactions of the royal society a: mathematical, physical and engineering sciences* 376 (2128): 20170357. https://doi.org/10.1098/rsta.2017.0357

MITRE. 2024. *Strategic Economics: Options for Competitive Advantage.* https://www.mitre.org/sites/default/files/2024-10/PR-%2024-2927-%20Lessons-Learned-From-NATO-Collaborative-Strategies.pdf

Naseem, A., S.T.H. Shah, S.A. Khan, and A.W. Malik. 2017. "Decision support system for optimum decision making process in threat evaluation and weapon assignment: Current status, challenges and future directions." *Annual reviews in control* 43: 169-187. https://doi.org/10.1016/j.arcontrol.2017.03.003

National Defense Magazine. 2025. *NATO on hunt for innovative defense tech.* https://www.nationaldefensemagazine.org/articles/2025/6/12/nato-on-hunt-for-innovative-defense-tech

Nelson, C., I. Adiguzel, M.V. Florin, F. Lentzos, R. Knutsson, C. Rhodes, ... and A. Vergin. 2021. "Foresight in synthetic biology and biotechnology threats." *Emerging threats of synthetic biology and biotechnology: addressing security and resilience issues*, 177-194. https://doi.org/10.1007/978-94-024-2086-9_12

Németh, B., N. Dew, and M. Augier. 2018. Dew, and M. Augier Understanding some pitfalls in the strategic foresight processes: The case of the Hungarian Ministry of Defense." *Futures* 101: 92-102. https://doi.org/10.1016/j.futures.2018.06.014

Onderco, M. 2025. "Navigating the AI frontier: Insights from the Ukraine conflict for NATO's governance role in military AI." *Journal of Strategic Studies* 48(3): 602-626. https://doi.org/10.1080/01402390.2025.2463451

Papanikolaou, A., A. Alevizopoulos, C. Ilioudis, K. Demertzis, and K. Rantos. 2023. "A Cyber Threat Intelligence Management Platform for Industrial Environments." *arXiv preprint arXiv:2301.03445*. https://doi.org/10.48550/arXiv.2301.03445

Park, S. 2023. "Bridging the global divide in AI regulation: a proposal for a contextual, coherent, and commensurable framework." *Wash. Int'l LJ* 33: 216. https://doi.org/10.48550/arxiv.2303.11196

Pataki, J. 2019. "NATO in 2030 and what the future will bring –'Essential security, dynamic engagement'." *Nemzetbiztonsági Szemle* 7(4): 61-70. https://doi.org/10.32561/nsz.2019.4.5

Pham, T. 2025. "Ethical and legal considerations in healthcare AI: innovation and policy for safe and fair use." *Royal Society Open Science* 12(5): 241873. https://doi.org/10.1098/rsos.241873

Porkoláb, I. 2020. "An AI Enabled NATO Strategic Vision for Twenty-First-Century Complex Challenges." In *Artificial Intelligence and Global Security* (pp. 153-165). Emerald Publishing Limited. https://doi.org/10.1108/978-1-78973-811-720201009

Reddy R.P. 2025. "Cyber Warfare: National Security Implications and Strategic Defense Mechanisms." *International Journal of Computer Trends and Technology (IJCTT)* 73(4): 48-59. https://doi.org/10.14445/22312803/ijctt-v73i4p107

Rizzo, F., F. Schmittinger, and A. Deserti, A. 2020. "Expanding innovation capacity in public sector by design projects." *Proceedings of DRS* 5: 1993-2009. https://doi.org/10.21606/drs.2020.355

Roberson, T., S. Bornstein, R. Liivoja, S. Ng, J. Scholz, and K. Devitt. 2022. "A method for ethical AI in defence: A case study on developing trustworthy autonomous systems." *Journal of Responsible Technology* 11: 100036. https://doi.org/10.48550/arxiv.2206.10769

Roorda, M. 2015. "NATO's Targeting Process: Ensuring Human Control Over and Lawful Use of 'Autonomous' Weapons." *Mark Roorda, NATO's Targeting Process: Ensuring Human Control Over (and Lawful Use of)'Autonomous' Weapons, in: Autonomous Systems: Issues for Defence Policymakers, eds. Andrew Williams and Paul Scharre, NATO Headquarters Supreme Allied Command Transformation, Amsterdam Center for International Law*, (2015-06). https://ssrn.com/abstract=2593697

Schiliro, F. 2023. "Building a resilient cybersecurity posture: a framework for leveraging prevent, detect and respond functions and law enforcement collaboration." *arXiv preprint arXiv:2303.10874*. https://doi.org/10.48550/arxiv.2303.10874

Schiuma, G., and D. Carlucci. 2018. "Managing strategic partnerships with universities in innovation ecosystems: A research agenda." *Journal of Open Innovation: Technology, Market, and Complexity* 4(3): 25. https://doi.org/10.3390/joitmc4030025

Schuett, J. 2023. "Risk Management in the Artificial Intelligence Act." *European Journal of Risk Regulation* 15(2): 367. https://doi.org/10.1017/err.2023.1

Shafiabady, N., N. Hadjinicolaou, F.U. Din, B. Bhandari, R. Wu, and J. Vakilian. 2023. "Using Artificial Intelligence (AI) to predict organizational agility." *Plos one* 18(5): e0283066. https://doi.org/10.1371/journal.pone.0283066

Sharma, D.N. 2024. "Artificial intelligence: Legal implications and challenges." *Knowledgeable Research A Multidisciplinary Journal* 2(11): 13-32. https://doi.org/10.57067/220k4298

Shiny, J.M. DrK. V., K. Rohith, C.B.R. Reddy and C. Ganesh. 2025. "AI Powered SOCs Detect and Respond to Cyber Security Threats in Real Time by using Deep Learning." *International Journal of Innovative Research in Science engineering and Technology* 14(4). https://philarchive.org/rec/DRKAPS

Slapakova, L., A. Fraser, M. Hughes, M.C. Aquilino, and K. Thue. 2024. *Cultural and technological change in the future information environment*. RAND. https://doi.org/10.7249/rra2662-1

Stanley-Lockman, Z. 2021. "Responsible and ethical military AI." *Centre for Security and Emerging Technology*. https://doi.org/10.51593/20200091

Taddeo, M., and A. Blanchard. 2023. "A comparative analysis of the definitions of autonomous weapons." In *The 2022 yearbook of the digital governance research group* (pp. 57-79). Cham: Springer Nature Switzerland. https://doi.org/10.1007/s11948-022-00392-3

Taddeo, M., and L. Floridi. 2018. "Regulate artificial intelligence to avert cyber arms race." *Nature* 556 (7701): 296-298. https://doi.org/10.1038/d41586-018-04602-6

Taddeo, M., D. McNeish, A. Blanchard, and E. Edgar. 2022. "Ethical principles for artificial intelligence in national defence." In *The 2021 Yearbook of the Digital Ethics Lab* (pp. 261-283). Cham: Springer International Publishing. https://doi.org/10.1007/s13347-021-00482-3

Tomada, L. 2022. "Start-ups and the Proposed EU AI Act: Bridges or Barriers in the Path from Invention to Innovation?." *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 13: 53.

Vincent, B. 2024. *NATO's innovation accelerator begins search for its second cohort.* https://defensescoop.com/2024/07/01/nato-innovation-accelerator-diana-begins-search-second-cohort/?utm_source=chatgpt.com

Wasilow, S., and J.B. Thorpe. 2019. "Artificial intelligence, robotics, ethics, and the military: A Canadian perspective." *Ai Magazine* 40(1): 37-48. https://doi.org/10.1609/aimag.v40i1.2848

Weerasinghe, R.N., and A.K.W. Jayawardane. 2019. "The Art of Crafting Actionable National Innovation Policy: The Case of Sri Lanka." *Journal of Economics and Business* 2(4). https://doi.org/10.31014/aior.1992.02.04.163

Wilkinson, M., and S. Jewell. 2017. "Defence requires Enterprise-Level Innovation: Using a Systems Approach to secure superior Value from Ideas." In *INCOSE International Symposium* 27(1): 87-101). https://doi.org/10.1002/j.2334-5837.2017.00347.x

Willows, M. 2025. *DIANA: NATO's Innovation Powerhouse Springs into Action.* https://ddrc.uk/diana-natos-innovation-powerhouse-springs-into-action/?utm_source=chatgpt.com

Wyatt, A. 2023. "Examining Supply Chain Risks in Autonomous Weapon Systems and Artificial Intelligence." *Applied Cybersecurity & Internet Governance* 2(1): 1-21. https://doi.org/10.60097/acig/162874

Young, T.D. 2019. "NATO's selective sea blindness." *Naval War College Review* 72(3): 12-39. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8041&context=nwc-review

Zhang, G., J. Sun, and Y. Sun. 2023. "Mapping interdisciplinary collaboration in music education: analysis of models in higher education across North America, Europe, Oceania, and Asia." *Frontiers in Psychology* 14: 1284193. https://doi.org/10.3389/fpsyg.2023.1284193

Zurek, T., J. Kwik, and T. Van Engers. 2023. "Model of a military autonomous device following International Humanitarian Law." *Ethics and Information Technology* 25(1): 15. https://doi.org/10.1007/s10676-023-09682-1

ACKNOWLEDGEMENTS

I express my gratitude to Professor Mehmet Ziya SÖĞÜT for his support and 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 on the internet.

DECLARATION on AI use (if applicable)

N/A

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Shielding Against Social Engineering Threats: A Counterintelligence Approach

Anastasios-Nikolaos KANELLOPOULOS, PhD Candidate*

*Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ankanell@aueb.gr

Abstract

In an increasingly networked global context, commercial counterintelligence units and competitive intelligence experts must deal with sophisticated social engineering threats that exploit human psychology rather than technological shortcomings. This article highlights the importance of counterintelligence training and robust security measures while analyzing the psychological manipulation tactics employed by adversaries to lower these risks.

The article examines social engineering strategies such as scarcity, authority, reciprocity, fear, and trust qualitatively to emphasize the significance of behavioral defenses and organizational awareness. The methodology, which evaluates institutional responses and psychological exploitation strategies, incorporates a review of the literature and expert comments. The paper's conclusion recommends a multi-layered approach that incorporates organizational cultural reforms, technical defenses, and psychological awareness to safeguard sensitive data from insider threats and social engineering.

Keywords:

Social Engineering; Counterintelligence; Human Psychology; Insider Threats; Security Awareness.

Article info

Received: 14 July 2025; Revised: 19 August 2025; Accepted: 15 September 2025; Available online: 6 October 2025

Citation: Kanellopoulos, A.N. 2025. "Shielding Against Social Engineering Threats: A Counterintelligence Approach." *Bulletin of "Carol I" National Defence University*, 14(3): 245-259. https://doi.org/10.53477/2284-9378-25-46

In today's intelligence environment, competitive intelligence has evolved from a reactive, market-focused discipline to a proactive function that shields companies from espionage, cyberthreats, and insider threats. In industries where economic competition and geopolitical conflicts collide, such as shipping, energy, and key infrastructure, the human element has become the most vulnerable entry point for adversaries. Conventional cyber defenses focus on technical safeguards, but in order to circumvent these barriers, adversaries are increasingly employing social engineering—the art of playing on people's emotions to get personal information or gain illegal access. This kind of attack is a significant problem for companies that have not adequately addressed the human dynamics that underlie their security architecture.

Social engineering attacks are effective because they exploit predictable psychological trends. Adversaries impersonate authority figures, exploit emotions like fear and trust, and generate urgency through scarcity. Additionally, they exploit the reciprocal social norm. By doing this, they circumvent rational barriers and trigger instinctive human responses that lead to the disclosure of personal information or the commission of criminal activity. Organizations that do not understand these psychological methods remain vulnerable, regardless of how advanced their technology is.

This article explores the connection between counterintelligence tactics, human psychology, and social engineering within the context of competitive intelligence. The primary objectives are to analyze how adversaries exploit psychological triggers and propose responses that combine technical controls with human awareness. The article uses a qualitative methodology and incorporates insights from the intelligence community, industry best practices, and academic literature.

The article also argues that a multipronged approach is required to counteract social engineering. Training and awareness efforts must first educate staff members about the psychological manipulation techniques employed by enemies. Second, human attention to detail must be used to supplement technical defenses with robust security measures, including encryption, anomaly detection systems, and extensive access controls. Third, systems that identify insider threats must monitor for any anomalous activity that could indicate an internal breach. Together, these protections offer a robust defense against human-centered attacks.

In the next chapters, the paper offers practical strategies for safeguarding sensitive data while also analyzing the evolving danger landscape of social engineering and breaking down the psychological concepts employed by adversaries. Through this complete analysis, the article highlights the value of counterintelligence training and a security-conscious company culture in mitigating human vulnerabilities, which remain the weakest link in the intelligence security chain.

The Intersection of Counterintelligence and Social Engineering

The Critical Importance of Counterintelligence

Counterintelligence (CI) is a crucial component of national security because it safeguards the sanctity of classified information, prevents foreign enemies from scheming, and maintains the integrity of national secrets (Shulsky and Schmitt 2009; Foryst 2010; Kanellopoulos 2024a). In an era of unprecedented global interconnectedness, where digital espionage and manipulation have become pervasive threats, social engineering has emerged as a significant challenge in the field of CI, which faces a constantly changing and complex landscape (Sims and Gerber 2009; Kuloğlu, Gül and Erçetin 2014; Barnea 2019). At its core, CI encompasses both offensive and defensive strategies, with counterespionage being a crucial component of the former. Understanding the intricate role of CI requires a further investigation of these components (Prunckun 2019; Kanellopoulos 2022).

Offensive CI is the proactive and strategic component of CI that focuses on identifying and removing threats from foreign intelligence agencies (FIS) and hostile organizations. The primary objective of offensive CI is to stop espionage activities that can endanger national security (Moyers 2025). This means learning the strategies and tactics that adversaries employ and using this knowledge to thwart their efforts. One essential element of offensive CI is counterespionage. Counterespionage, which includes a wide range of activities, is frequently seen as the first line of defense against spies. This means conducting operations to track down foreign operatives, keeping tabs on their movements, and learning about the methods and techniques used by enemy intelligence services. Double-agent operations, which involve convincing a foreign spy to join the host country's intelligence service, are another tactic offensive counterintelligence agents may use to turn the tables on the enemy (Stouder and Gallagher 2013).

Additionally, defensive CI strengthens the offensive components by focusing on preventing illegal access and exfiltration of sensitive information and classified data (Johnson 2010). It entails proactively and thoroughly identifying the national security apparatus's flaws (Sithole and Du Toit 2022). Defensive CI includes digital and physical security measures as well as personnel security protocols. In the subject of defensive CI, countermeasures against social engineering are essential. Salama and Fadi Al-Turjman (2023) define social engineering as the act of deceiving someone into divulging personal information or permitting unauthorized access. It frequently involves psychological manipulation, deception, and the exploitation of human emotions such as trust and fear. Because social engineering can occur both in person and online, it is a challenging problem in this age of advanced technology (Reynolds 2016; Hatfield 2018). In the modern era, the line between physical and digital security has blurred, and CI needs to adapt to a changing and connected landscape. The ability to anticipate and respond to foreign opponents' evolving tactics is essential. In addition to a commitment to safeguarding national secrets, this necessitates a blend of technology expertise, strategic planning, and human intelligence (Reynolds 2016).

Social Engineering as a Gateway

A significant risk to national security, social engineering is a strong and secretive technique that has emerged as a key entrance point for espionage operations. Adversaries that are adept in psychological manipulation and dishonest techniques employ this tactic to get illegal access to sensitive information, exploit vulnerabilities, and eventually endanger a nation's security (Breda, Barbosa and Morais 2017). These sophisticated attacks typically target specific persons within an organization since humans are typically regarded as the weakest link in the security chain. At its fundamental level, social engineering is a form of manipulation that relies on human psychology and trust (Reynolds 2016; Hadnagy 2018). It can take many different forms and be done both in the actual and digital worlds. Influencing people to reveal personal information or perform actions they wouldn't often consider taking is the primary goal of social engineering assaults. Cybercriminals can obtain illegal access to computer systems and sensitive data by revealing passwords, allowing access to secure areas, or clicking on harmful links in emails (Hatfield 2018; Syafitri, et al. 2022).

Furthermore, social engineers are skilled at exploiting traits and tendencies that are common to all people, such as curiosity, trust, fear, and the desire to be helpful (Reynolds 2016; Hadnagy 2018). They can pose as trustworthy colleagues, IT support personnel, or even superiors like auditors or police enforcement. By employing these personas to build rapport and trust, they can more readily persuade their targets to violate security protocols (Matyokurehwa, et al. 2022). The social engineering method known as "phishing" is widely used. Phishing attempts often use convincingly fake emails that look real. These emails persuade recipients to give personal information, download dangerous files, or click on links that lead to malicious websites. Such assaults can have catastrophic consequences since they have the potential to undermine whole networks and the integrity of a nation's sensitive data (Bhavsar, Kadlak and Sharma 2018).

Eventually, social engineering is particularly harmful because it does not call for sophisticated hacking tools or technological know-how (Gray 2021). Instead, it makes use of human nature and the inclination for people to believe in and assist others. This makes it challenging to fight against, as traditional cybersecurity technologies like firewalls and antivirus software often fail to stop these attacks. In each organization's security chain, people are typically the weakest link (Reynolds 2016; Hadnagy 2018).

The Anatomy of Social Engineering Attacks

The Spectrum of Social Engineering Attacks

Adversaries now employ a wide variety of effective strategies, including social engineering assaults, to trick people into inadvertently exposing personal information and jeopardizing security (Erbschloe 2020). These approaches, which exploit human psychology, trust, and vulnerabilities, are typical of a range of

strategies used by adversaries in the digital age (Reynolds 2016; Hadnagy 2018). It is necessary to comprehend this spectrum in order to strengthen defenses against these cunning attacks.

Phishing is a prevalent social engineering tactic whereby thieves send phony emails or messages purporting to be banks or reputable companies in an attempt to steal private information, such as financial information or passwords (Bhavsar 2018). By creating a sense of urgency or panic, such as notifications about hacked accounts or past-due payments, these attacks usually use psychological pressure to cause victims to act rashly (Wang and Lutchkus 2023). Phishing typically involves harmful links or attachments that direct users to fake websites that appear real in order to gain login credentials or personal information (Sharma, Dash and Ansari 2022). Once they have access, hackers may commit fraud, identity theft, or other cyberattacks. For victims, money losses, data breaches, and reputational harm are serious consequences.

Furthermore, impersonation is a social engineering strategy whereby attackers pose as trustworthy individuals or organizations in order to exploit people's confidence, according to Algarni et al. (2013). In order to fool victims into responding with bogus demands, attackers pose as trustworthy companies, family members, or coworkers (Reynolds 2016; Almomani and Alauthman 2025). Attackers may use organizational hierarchy and trust to pretend to be superiors or coworkers in the workplace and request private information, like login passwords or financial information, over the phone or by email. Similarly, family-friend impersonators use emotional attachments and often fabricate crises to pressure victims into divulging personal information (Jakobsson 2018). Impersonation can also target customers through honey emails, websites, or phone calls from tech companies, banks, or government agencies. By employing compelling language, realistic logos, and stolen personal information, attackers establish urgency and believability, which prompts victims to take immediate action. Successful impersonation requires establishing confidence and capitalizing on the victim's innate desire to cooperate or assist.

Subsequently, in elicitation, attackers might utilize a subtle social engineering approach called elicitation to get sensitive information through casual conversation, as an alternative to overt tactics like phishing or impersonation (Cooke 1994). It exploits people's natural inclination toward open communication and trust (Beckers and Pape 2016). As they appear kind and unthreatening, attackers often initiate harmless talks in social or professional settings and then gradually steer the conversation toward their target information (Beckers, et al. 2017). Leading inquiries, active listening, and reciprocal sharing are some of the tactics they use to encourage disclosure and build trust. Elicitation is especially effective in situations where informal trust develops, such as social events, networking groups, or professional settings where individuals may share project, commercial, or private information without fully comprehending the hazards (Tiwari and Rathore 2017).

In addition, pretexting is the act of creating fake situations or events to pressure someone into sharing personal information. The attackers fabricate a story that sounds plausible by using a pretext that appeals to the target's emotions or aspirations. This could entail posing as a financial institution conducting a major audit or a colleague in need of assistance. These made-up scenarios compel people to reveal personal information or take actions that compromise their security (Alazri 2015).

Finally, tailgating is a physical social engineering approach that allows attackers to access secure facilities without authorization by exploiting human kindness or negligence (Sobur, et al. 2024). Unlike digital attacks, it circumvents security mechanisms by using human behavior and physical presence. When following an authorized individual via a secure entry, the attacker frequently blends in by dressing appropriately or carrying materials that appear professional in order to allay suspicions (Cheh et al. 2019). Because they think anyone in the area should be there, victims may leave the door open without verifying credentials out of courtesy or to avoid confrontation. Tailgating is prevalent in safe establishments, such as offices, where people are rushing or willing to assist. One of the risks of a successful attack is unauthorized access to sensitive areas, which could lead to data breaches or other security issues.

Exploiting Human Psychology

In the discipline of CI, understanding the psychology of social engineering is essential. A wide range of psychological ideas is commonly employed by skilled manipulators to execute their covert operations. Understanding these psychological techniques is necessary to develop effective defenses against social engineering threats (Schaab, Beckers and Pape 2017).

One of the core psychological ideas used by social engineers is authority. Adversaries typically assume the identities of authoritative individuals, such as law enforcement, senior executives, or trustworthy supervisors, in order to pressure others into meeting their demands. People's natural inclination to defer to and obey those in power can be leveraged to promote cooperation and the sharing of personal information. Because it may overcome skepticism and critical thinking simply by existing, perceived authority is a potent tool in the social engineer's toolkit (Bullée, et al. 2017).

Reciprocity is another psychological idea that enemies exploit. People frequently feel obliged to repay others when they get something beneficial or a favor. Social engineers exploit this tendency to persuade others by presenting what seems to be a benefit. Giving creates a sense of duty in the recipient, which frequently results in them returning the favor by granting access or disclosing personal information. This is true whether the present is little, a gesture of appreciation, or an informational nugget. This approach takes advantage of people's innate desire to maintain fair and balanced social relationships (Bullée, et al. 2015).

In addition, instilling a sense of urgency or scarcity is another psychological tactic social engineers employ to suppress reason. When people think a resource or opportunity is limited or in great demand, they are more likely to act impulsively. Adversaries use this sense of urgency by imposing false restrictions or time constraints on their targets. For example, they could pose as a trustworthy source and threaten to delete the user's account if they do not provide information immediately. Fear of losing out or the potential consequences of delay might cause people to act hastily, ignoring their usual caution and skepticism (Siddiqi, Pak and Siddiqi 2022).

The delicate interplay between trust and fear is a psychological tactic that adversaries utilize to obtain personal information. By inciting fear, usually through threats or terrifying scenarios, social engineers can make people feel more pressured and nervous. In this state, they are more inclined to act irrationally, which may involve divulging personal information, in an attempt to reduce perceived risks. However, trust is another tool used by social engineers to build rapport and sway their victims. When people believe they are communicating with a trustworthy person or thing, their guard is down and they are more susceptible to manipulation. A fundamental human need is trust (Siddiqi, Pak and Siddiqi 2022).

Strategies to Safeguard Against Social Engineering Threats

Counterintelligence Training

Increasing their defenses against the crafty and misleading tactics of social engineering is a more crucial task for counterintelligence agencies and companies in a time when cyber threats are increasing and the area of espionage and subterfuge is continuously evolving. In this ongoing battle, training and awareness programs are essential because they equip employees with the knowledge and skills necessary to identify, repel, and overcome these threats (Kanellopoulos 2023).

Identifying Typical Social Engineering Strategies: One of the main tenets of CI training is to help employees recognize common social engineering strategies. Phishing, impersonation, elicitations, pretexting, and tailgating are some of the tactics used to deceive people into breaking security protocols or divulging personal information. Training programs must teach participants how to spot the warning signs of these tactics, which include suspicious emails, strange demands, or people acting differently from their typical behavior. By raising awareness of the intricate nature of social engineering, organizations can cultivate a vigilant and informed staff (Aldawood and Skinner 2018).

Performing Simulated Exercises: CI training includes both theoretical and practical application. Simulations are a great way to test how employees respond to social engineering attempts in real-world scenarios. These exercises assist firms in evaluating how well-trained and equipped their staff are by mimicking enemy tactics. By simulating phishing assaults, impersonation scenarios, and other forms

of social engineering, organizations can identify areas for development, evaluate the efficacy of their defenses, and adjust their training. These exercises not only evaluate personal knowledge but also foster a culture of readiness (Banjo 2024).

Promoting a Culture of Skepticism: CI training should be used to establish a culture of skepticism among employees. The importance of verifying sensitive requests and actions cannot be overstated. People must be encouraged to seek affirmation, ask questions, and restrain their initial impulses when confronted with unfamiliar or potentially hazardous circumstances. This culture of skepticism is a basic protection against social engineering since it raises the bar for manipulation. It enables employees to act as the first line of defense against potential risks by exercising caution and critical thinking (Kanellopoulos 2022).

Educating Information Value: In order for employees to comprehend the significance of safeguarding sensitive data, they must be educated regarding the value of the data they handle. Understanding the consequences of compromised information goes beyond knowledge and fosters a sense of responsibility and commitment to national security. People who are aware of the potential consequences of data breaches are more likely to take their duties seriously and exercise caution when asked for sensitive information (Eminağaoğlu, Uçar, and Eren 2009).

Robust Security Protocols

Modern organizations seeking to protect their sensitive data and preserve the integrity of their operations must establish robust security protocols. These procedures incorporate a range of measures, from comprehensive security rules to state-of-the-art technology solutions, to mitigate the dangers associated with social engineering threats (Poehlmann 2021).

Comprehensive Security Policies and Procedures: The foundation of a strong security infrastructure is the development and application of comprehensive security policies and procedures. These documents serve as the cornerstone of an organization's security plan. They define best practices for security, provide protocols for handling sensitive data, and outline the duties and obligations of employees. Additionally, they ought to go over the dangers of social engineering tactics and provide detailed guidance on how to recognize and deal with them. An educated and informed staff is essential to these policies because it ensures that employees can recognize and stop dishonest practices (Chen, Ramamurthy and Wen 2019).

State-of-the-Art Intrusion Detection Systems and Firewalls: To improve their defenses against social engineering, organizations need to deploy state-of-the-art intrusion detection systems and firewalls. These technologies are the first line of protection against internet threats such as malware, phishing schemes, and unauthorized access attempts. Through constant network traffic scanning for anomalous activity, intrusion detection systems promptly alert security professionals

to potential threats. Firewalls serve as a barrier between trusted internal networks and untrusted external networks by blocking unauthorized access and eliminating potentially dangerous material. Together, these solutions offer a proactive and reactive security posture to stop and mitigate the impact of social engineering (Anwar 2017).

Two-Factor Authentication (2FA): To enhance access control and lessen the likelihood of unwanted access to sensitive systems and data, organizations ought to require two-factor authentication (2FA). 2FA adds a layer of security by combining two different authentication methods to verify the identity of individuals seeking access. This typically involves both a user-known object (such as a password or PIN) and a user-possessed item (such as a security token or smartphone). By implementing 2FA, organizations significantly reduce the likelihood that social engineers would get access through credential theft or impersonation. Even if an attacker manages to obtain a password, they will still need the second factor to obtain access (Wang and Wang 2016).

Investment in Encryption Tools: Particularly in the event of a breach, encryption is crucial for avoiding unauthorized access to private data. When information is converted into a code that can only be decoded by those with the required encryption keys, it is said to be encrypted. This ensures that even if an attacker can access the data, it is worthless and unintelligible without the decryption key. Because encryption techniques offer an additional layer of safety and render any stolen or intercepted data incomprehensible, they are essential for both data in transit and data at rest. This safeguard is particularly important when managing classified or highly sensitive information since it stops data from being abused in the event of a social engineering assault (Volini 2021).

Insider Threat Detection

Since CI methods currently recognize that internal risks can jeopardize an organization's security, it is imperative to comprehend and identify insider threats in order to protect sensitive data. Insider risks can occur when employees, contractors, or even trusted individuals intentionally breach security by abusing their access. In many cases, social engineering approaches enable these risks. To handle this pressing challenge, organizations need to employ a range of strategies and tools to actively monitor and mitigate these risks (Kanellopoulos 2024b).

Techniques for Recognizing Odd or Suspicious Behavior: The first line of defense against insider threats is putting in place systems to spot odd or suspicious conduct among staff members. Since these systems recognize that insider threats are not necessarily the result of malicious intent, they focus on identifying deviations from normal behavior. An employee who suddenly accesses an unusual amount of data, tries to circumvent security measures, or exhibits irregular work habits, for example, may be exhibiting signs of an insider threat (Georgiadou, Mouzakitis and Askounis

2021). Behavioral analytics tools can be used to monitor user activity and spot deviations from established patterns. This allows companies to respond swiftly to unusual conduct, whether it is the product of a malicious insider or an inadvertent participant in a social engineering fraud (Cho and Lee 2016).

Employee Monitoring and Auditing Systems: To keep up their proactive approach to spotting insider threats, organizations might use employee monitoring and auditing systems. These technologies provide continuous monitoring of digital activity, including file access, system logins, and data transfers (Subhani, Khan and Zubair 2021). By collecting and examining these records, organizations can identify unusual conduct and look into it further. These devices serve as a deterrent as well as a tool for danger identification since workers are aware that their actions are being observed. Knowing that their activities are being observed deters social engineers, and malicious insiders are less likely to act covertly as a result of this monitoring (Stavrou, et al. 2014).

Extensive Background Checks and Personnel Vetting: The first line of defense against insider threats is thorough personnel vetting, which includes extensive background checks for anyone with access to sensitive information. These checks should include a detailed examination of an individual's qualifications, employment history, and criminal background, if any (Beneda and Jaros 2020). Background checks also take into account a person's financial history, connections, and contacts that could influence their loyalty or susceptibility to social engineering tactics. This comprehensive screening process is crucial for identifying any red flags or potential vulnerabilities that adversaries could take advantage of. By using background checks, organizations can lower the risk of insiders who could jeopardize their security (Alsowail and Al-Shehari 2021).

Conclusion

In a modern intelligence and security environment, social engineering is one of the most dangerous and underestimated risks that enterprises must contend with. Despite advancements in cybersecurity technologies, adversaries continue to target the human element, which is the most unpredictable and vulnerable component of any security system. This article has shown how social engineers exploit fundamental psychological ideas like authority, reciprocity, scarcity, fear, and trust to get beyond rational defenses and force people to provide personal information.

Countering these attacks requires a change in viewpoint from solely technical defenses to an integrated security approach, where CI is crucial. Training programs that educate employees about the tactics and psychological manipulation techniques used by social engineers are essential to developing an educated and resilient workforce. However, training alone is not enough. Organizations must implement a wide range of security measures as a contingency in case human attention is

insufficient, including intrusion detection systems, encryption software, and strong authentication methods.

In addition, the growing danger of insider threats, whether deliberate or inadvertent, highlights the need for constant behavioral surveillance, stringent recruiting procedures, and the creation of a security-focused corporate culture. Social engineering assaults are often facilitated by insider threats, who either work directly with adversaries or inadvertently enable breaches through careless behavior.

Ultimately, to safeguard sensitive data in high-risk industries like transportation, energy, and vital infrastructure, companies must acknowledge that human psychology is both a vulnerability and a defense mechanism. By predicting how attackers exploit psychological triggers, organizations can reduce their exposure to intelligence threats and proactively protect against social engineering. The article's findings emphasize that social engineering is a basic counterintelligence problem, not just a cybersecurity one, and that it calls for an all-encompassing strategy that incorporates continuous attention to detail, technology restrictions, and training. Fundamentally, the battle against social engineering is ongoing, adaptable, and psychological. Companies that invest in understanding and addressing this issue will be better able to protect their national security interests, competitive advantage, and operational integrity in an increasingly complex intelligence environment.

References

Alazri, A. S. 2015. "The Awareness of Social Engineering in Information Revolution: Techniques and Challenges." In *2015, the 10th International Conference for Internet Technology and Secured Transactions (ICITST)*. https://doi.org/10.1109/icitst.2015.7412088.

Aldawood, H., and G. Skinner. 2018. "Educating and Raising Awareness on Cyber Security Social Engineering: A Literature Review." In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, 62–68. https://doi.org/10.1109/tale.2018.8615162.

Algarni, A., Y. Xu, Taizan Chan, and Yu-Chu Tian. 2013. "Social Engineering in Social Networking Sites: Affect-Based Model." In *8th International Conference for Internet Technology and Secured Transactions (ICITST-2013)*. https://doi.org/10.1109/icitst.2013.6750253.

Almomani, A., and M. Alauthman. 2025. *Examining Cybersecurity Risks Produced by Generative AI*. IGI Global.

Alsowail, R. A., and T. Al-Shehari. 2021. "A Multi-Tiered Framework for Insider Threat Prevention." *Electronics* 10 (9): 1005. https://doi.org/10.3390/electronics10091005.

Anwar, S., J. Mohamad Zain, M. F. Zolkipli, Z. Inayat, S. Khan, B. Anthony, and V. Chang. 2017. "From Intrusion Detection to an Intrusion Response System: Fundamentals, Requirements, and Future Directions." *Algorithms* 10 (2): 39. https://doi.org/10.3390/a10020039.

Banjo, O. 2024. "Enhancing Cybersecurity through Comprehensive User Training Programs: A Study on Mitigating Social Engineering Threats." *NORMA@NCI Library*. https://norma.ncirl.ie/7734/1/olumideoladapobanjo.pdf.

Barnea, A. 2019. "Big Data and Counterintelligence in Western Countries." *International Journal of Intelligence and CounterIntelligence* 32 (3): 433–447. https://doi.org/10.1080/08850607.2019.1605804.

Beckers, K., and S. Pape. 2016. "A Serious Game for Eliciting Social Engineering Security Requirements." https://mediatum.ub.tum.de/doc/1328974/1328974.pdf.

Beckers, K., V. Fries, E. Groen, and S. Pape. 2017. "Creativity Techniques for Social Engineering Threat Elicitation: A Controlled Experiment." https://ceur-ws.org/Vol-1796/creare-paper-1.pdf.

Beneda, J., and S. L. Jaros. 2020. "The PAR Capabilities and the Convergence of Workplace Violence Prevention, Counter-Insider Threat, and Personnel Vetting Policies in DoD." https://apps.dtic.mil/sti/html/tr/AD1094489/index.html.

Bhavsar, V., A. Kadlak, and S. Sharma. 2018. "Study on Phishing Attacks." *International Journal of Computer Applications* 182 (33): 27–29. https://www.ijcaonline.org/archives/volume182/number33/30244-2018918286/.

Breda, F., H. Barbosa, and T. Morais. 2017. "Social Engineering and Cyber Security." *INTED2017 Proceedings* 1: 4204–4211. https://www.scirp.org/reference/referencespapers?referenceid=3347298.

Bullée, J. W. H., L. Montoya, W. Pieters, M. Junger, and P. H. Hartel. 2015. "The Persuasion and Security Awareness Experiment: Reducing the Success of Social Engineering Attacks." *Journal of Experimental Criminology* 11 (1): 97–115. https://doi.org/10.1007/s11292-014-9222-7.

___. 2017. "On the Anatomy of Social Engineering Attacks—A Literature-Based Dissection of Successful Attacks." *Journal of Investigative Psychology and Offender Profiling* 15 (1): 20–45. https://doi.org/10.1002/jip.1482.

Cheh, C., U. Thakore, B. Chen, W. Temple, and W. Sanders. 2019. "Leveraging Physical Access Logs to Identify Tailgating: Limitations and Solutions." https://www.perform.illinois.edu/Papers/USAN_papers/19CHE01.pdf.

Chen, Y., K. Ramamurthy, and K. W. Wen. 2019. "Impacts of Comprehensive Information Security Programs on Information Security Culture." *Journal of Computer Information Systems* 55 (3): 11–19. https://doi.org/10.1080/08874417.2015.11645767.

Cho, I., and K. Lee. 2016. "Advanced Risk Measurement Approach to Insider Threats in Cyberspace." *Intelligent Automation & Soft Computing* 22 (3): 405–413. https://doi.org/10.1080/10798587.2015.1121617.

Cooke, N. J. 1994. "Varieties of Knowledge Elicitation Techniques." *International Journal of Human-Computer Studies* 41 (6): 801–849. https://doi.org/10.1006/ijhc.1994.1083.

Eminağaoğlu, M., E. Uçar, and Ş. Eren. 2009. "The Positive Outcomes of Information Security Awareness Training in Companies – A Case Study." *Information Security Technical Report* 14 (4): 223–229. https://doi.org/10.1016/j.istr.2010.05.002.

Erbschloe, M. 2020. *Social Engineering: Hacking Systems, Nations, and Societies*. CRC Press, Taylor & Francis Group.

Foryst, C. A. 2010. "Rethinking National Security Strategy Priorities." *International Journal of Intelligence and CounterIntelligence* 23 (3): 399–425. https://doi.org/10.1080/08850600903566165.

Georgiadou, A., S. Mouzakitis, and D. Askounis. 2021. "Detecting Insider Threat via a Cyber-Security Culture Framework." *Journal of Computer Information Systems* 62 (4): 1–11. https://doi.org/10.1080/08874417.2021.1903367.

Gray, J. 2021. *Practical Social Engineering: A Primer for the Ethical Hacker*. San Francisco: No Starch Press.

Hadnagy, C. 2018. *Social Engineering: The Science of Human Hacking*. Indianapolis, IN: Wiley.

Hatfield, J. M. 2018. "Social Engineering in Cybersecurity: The Evolution of a Concept." *Computers & Security* 73: 102–113. https://doi.org/10.1016/j.cose.2017.10.008.

Jakobsson, M. 2018. *Understanding Social Engineering Based Scams*. Cham: Springer.

Johnson, L. K. 2010. *Handbook of Intelligence Studies*. London: Routledge.

Kanellopoulos, A. N. 2022. "The Importance of Counterintelligence Culture in State Security." *Global Security and Intelligence Note* 1 (5). https://www.buckingham.ac.uk/research/bucsis/hub/gsin/library/.

___. 2023. "The Dimensions of Counterintelligence and Their Role in National Security." *Journal of European and American Intelligence Studies* 6 (2).

___. 2024a. "Counterintelligence, Artificial Intelligence and National Security: Synergy and Challenges." *Journal of Politics and Ethics in New Technologies and AI* 3 (1): e35617–e35617. https://doi.org/10.12681/jpentai.35617.

__. 2024b. "Insider Threat Mitigation through Human Intelligence and Counterintelligence: A Case Study in the Shipping Industry." *Defense and Security Studies* 5: 10–19. https://doi.org/10.37868/dss.v5.id261.

Kuloğlu, G., Z. Gül, and Ş. Ş. Erçetin. 2014. "Counter-Intelligence as a Chaotic Phenomenon and Its Importance in National Security." In *Understanding Complex Systems*, 171–88. https://doi.org/10.1007/978-94-017-8691-1_11.

Matyokurehwa, K., N. Rudhumbu, C. Gombiro, and C. Chipfumbu-Kangara. 2022. "Enhanced Social Engineering Framework Mitigating against Social Engineering Attacks in Higher Education." *Security and Privacy*. https://doi.org/10.1002/spy2.237.

Moyers, R. 2025. "Deconstructing and Reconstructing Strategic Counterintelligence Toward a New Model." *Studies in Intelligence* 69 (2). https://www.cia.gov/resources/csi/static/Article-Moyers-Strategic-Counterintelligence-June-2025-1.pdf.

Poehlmann, N., K. M. Caramancion, I. Tatar, Y. Li, M. Barati, and T. Merz. 2021. "The Organizational Cybersecurity Success Factors: An Exhaustive Literature Review." In *Advances in Security, Networks, and Internet of Things*, 377–95. https://doi.org/10.1007/978-3-030-71017-0_27.

Prunckun, Harry. 2019. *Counterintelligence Theory and Practice*. Rowman & Littlefield.

Reynolds, Vincent. 2016. *Social Engineering: The Art of Psychological Warfare, Human Hacking, Persuasion & Deception*. Createspace.

Salama, R., and Fadi Al-Turjman. 2023. "Cyber-Security Countermeasures and Vulnerabilities to Prevent Social-Engineering Attacks." In *CRC Press EBooks*, 133–44. https://doi.org/10.1201/9781003322887-7.

Schaab, Philipp, Karsten Beckers, and Sebastian Pape. 2017. "Social Engineering Defence Mechanisms and Counteracting Training Strategies." *Information and Computer Security* 25 (2): 206–22. https://doi.org/10.1108/ics-04-2017-0022.

Sharma, Prakash, Bibhudutta Dash, and Mohammed F. Ansari. 2022. "Anti-Phishing Techniques – A Review of Cyber Defense Mechanisms." *Social Science Research Network*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4335354.

Shulsky, Abram N., and Gary J. Schmitt. 2009. *Silent Warfare: Understanding the World of Intelligence*. Potomac Books, Inc.

Siddiqi, Muhammad A., Won Pak, and Muhammad A. Siddiqi. 2022. "A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures." *Applied Sciences* 12 (12): 6042. https://doi.org/10.3390/app12126042.

Sims, Jennifer E., and Burton L. Gerber. 2009. *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence*. Center for Peace and Security Studies – Georgetown University Press.

Sithole, Themba, and Johann Du Toit. 2022. "A Cyber Counterintelligence Competence Framework." *European Conference on Cyber Warfare and Security* 21 (1): 368–77. https://doi.org/10.34190/eccws.21.1.255.

Sobur, Abdus, A. Hossain, Kazi Nazrul Islam, and Md Humayun Kabir. 2024. "A Contradistinction Study of Physical vs. Cyberspace Social Engineering Attacks and Defense." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4878111.

Stavrou, Vasilis, Michalis Kandias, Georgios Karoulas, and Dimitris Gritzalis. 2014. "Business Process Modeling for Insider Threat Monitoring and Handling." In *Trust, Privacy, and Security in Digital Business*, 119–31. https://doi.org/10.1007/978-3-319-09770-1_11.

Stouder, Michael D., and Sean Gallagher. 2013. "Crafting Operational Counterintelligence Strategy: A Guide for Managers." *International Journal of Intelligence and CounterIntelligence* 26 (3): 583–96. https://doi.org/10.1080/08850607.2013.780560.

Subhani, A., I. A. Khan, and A. Zubair. 2021. "Review of Insider and Insider Threat Detection in the Organizations." *Journal of Advanced Research in Social Sciences and Humanities* 6 (4). https://doi.org/10.26500/jarssh-06-2021-0402.

Syafitri, W., Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim. 2022. "Social Engineering Attacks Prevention: A Systematic Literature Review." *IEEE Access* 10 (1): 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594.

Tiwari, S., and S. S. Rathore. 2017. "A Methodology for the Selection of Requirement Elicitation Techniques." arXiv. https://arxiv.org/abs/1709.08481.

Volini, A. 2021. "A Deep Dive into Technical Encryption Concepts to Better Understand Cybersecurity & Data Privacy Legal & Policy Issues." *Digital Commons @ University of Georgia School of Law*. https://digitalcommons.law.uga.edu/jipl/vol28/iss2/2/.

Wang, D., and P. Wang. 2016. "Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound." *IEEE Transactions on Dependable and Secure Computing* 15 (4). https://doi.org/10.1109/tdsc.2016.2605087.

Wang, P., and P. Lutchkus. 2023. "Psychological Tactics of Phishing Emails." *Issues in Information Systems* 24 (2). https://doi.org/10.48009/2_iis_2023_107.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Perspectives Regarding UAS Control in Aquatic Environments (Rivers and Streams) based on Machine Learning

Lt. Cosmin-Alin MIRCEA*

*Ministry of National Defense, Romania
e-mail: srg_cosminalin@yahoo.com

Abstract

In recent years, the integration of artificial intelligence (AI) and machine learning (ML) in unmanned aerial systems (UAS) has led to increased decision-making autonomy, particularly in complex and dynamic environments. This study proposes an innovative framework for the autonomous operation of UAVs in aquatic scenarios, focusing on the continuous surveillance of a moving vessel. The system uses data from multiple sensors to allow a UAV to stay within a defined perimeter around the vessel, maintain stability above the water, and automatically land on a mobile platform when necessary (e.g., in case of low battery or interference). The decision-making architecture is based on reinforcement learning algorithms for flight control and drone replacement management. The contribution of this study is to propose an intelligent and modular model for the coordination of multi-UAV systems for river missions, with direct applications in surveillance, search and rescue, and environmental monitoring.

Keywords:
Machine Learning; Unmanned Aerial System (UAS); Artificial Intelligence; Aquatic Environments; Sensors.

Article info
Received: 14 August 2025; Revised: 1 September 2025; Accepted: 11 September 2025; Available online: 6 October 2025

Citation: Mircea, C.A. 2025. "Perspectives Regarding UAS Control in Aquatic Environments (Rivers and Streams) based on Machine Learning." *Bulletin of "Carol I" National Defence University*, 14(3): 260-277. https://doi.org/10.53477/2284-9378-25-47

With the engineering and technological development of various equipment or devices, unmanned aerial vehicles (UAVs), by their value, are relevant capabilities for many fields or purposes: agriculture, defense, search and rescue missions, etc. By visualizing and researching certain multidisciplinary aspects, the potential optimizations of any product or set of products can be identified. By connecting them within a network, they can communicate efficiently, quickly, and interchangeably, thus providing an essential and secure tool for practicing decision-making management and successfully conducting operations.

The operation of drones in both marine environments is difficult owing to platform (boat) movement, signal instability, weather conditions, and energy limitations. The problem is how we can ensure the continuous presence of an active drone in the air above a boat, maintaining it within a defined perimeter, with automatic localization and landing, as well as automatic replacement in various situations, based on artificial intelligence and autonomous decision management. To address this situation, the following aspects must be analyzed, as shown in the figure below (Figure 1) and as the authors Hassanalian M. and Abdelkefi A. (2017) also mention.

They can be used in areas such as those mentioned above, more specifically for fluvial or maritime surveillance for illegal fishing, smuggling, or national security. For search and rescue at sea, this solution of continuity based on machine learning can be critical in saving human lives. In addition, for environmental monitoring and protection purposes, this system can be used to collect data, such as temperature and the presence of pollutants, based on embedded sensors.
Finally, such a system can be used as a relay node between the ground and the boat, ensuring communication between the two stations in a redundant manner.

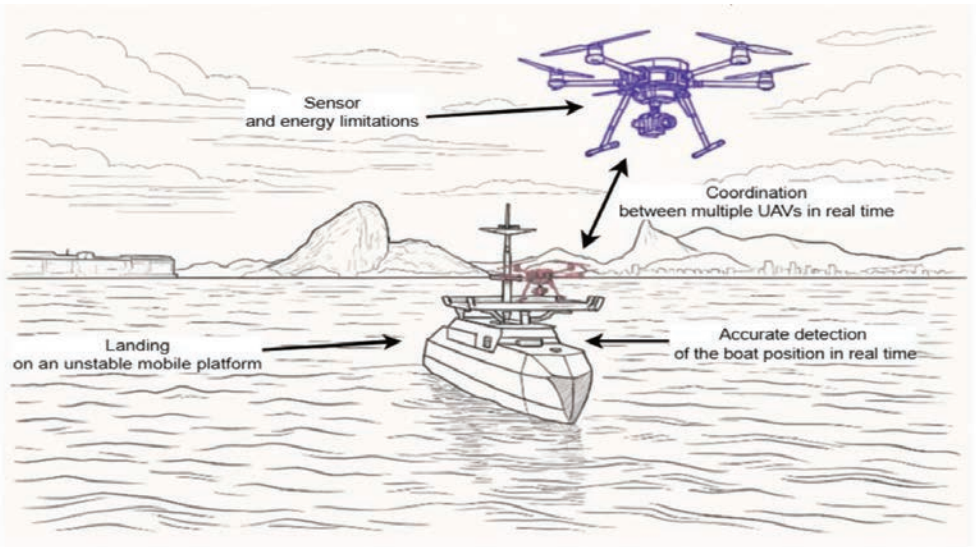

Figure 1 Major obstacles regarding the control of UAS in an aquatic environment
Source: adapted from https://static.wixstatic.com/media/bca94f_496a78a2fa3a4697a9cfc8eb4222ad5a~mv2.jpeg/v1/fill/w_748,h_606,al_c,q_85,usm_0.66_1.00_0.01,enc_avif,quality_auto/bca94f_496a78a2fa3a4697a9cfc8eb4222ad5a~mv2.jpeg

By studying the available literature and focusing on the latest information, this study explores the application of Machine Learning (ML) and Artificial Intelligence (AI) to enhance UAS control and autonomy within riverine domains, with a special focus on coordination, fault tolerance, and mission continuity.

The paper is structured as follows: introduction, state of the art (literature review), methodology – the framework and conceptual basis –, results and discussion – theory analysis and future work –, and conclusions. The research will contribute to the next steps towards practical simulations, using low-cost UAV devices that are software and hardware-configurable and capable of ML.

1. State of the Art

Analyzing the specialized literature on the subject, it is observed that the issue raised is of major interest among the authors, especially when we consider the evolution of the geopolitical space at a global level, where UAV systems are increasingly used. In current conflicts, drones have proven to be a very effective means of combat, substituting the human factor. From the Network-Centric Warfare (NCW) doctrine, a new current doctrine has emerged, centered on drones, which the Ukrainian Army is implementing by creating company-level combat subunits and even battalion-level units with a specific focus on drone strikes, within combat brigades (Samus 2024, 9).

The authors Wu L., Wang C., Zhang P., and Wei C. (2022) provide a comprehensive analysis of how reinforcement learning (RL) can be applied to enhance the coordination of UAVs based on corrective feedback, thus focusing on improving autonomous landing on mobile platforms (Song 2022). The aforementioned aspects are essential for network coordination in aquatic environments, where manual intervention is usually impossible. The RL method can ensure confidentiality and reduce latency (Chellapandi, et al. 2023, 3-6; Jung, et al. 2024, 1-23; Negru, et al. 2024, 1-23) – an important aspect regarding the security of UAVs, as well as operating them in unfriendly environments, where connection fluctuations may occur.

A study that addresses the visual challenges specific to the maritime environment (e.g., water reflections) and irregular target movements demonstrates that convolutional neural networks (CNN) can be used by a UAV swarm to successfully track certain targets (Zhao, et al. 2024, 3-18; Maharjan, et al. 2022, 1-24) while the study *"A Survey on UAV-Aided Maritime Communications: Deployment Considerations, Applications, and Future Challenges*" (Nomikos, et al. 2023, 56-78) analyzes the use of UAVs as aerial nodes in maritime communications through trajectory optimization and the use of ML for resource management and edge caching. This is highly relevant for UAVs in hostile environments, where connectivity requires adaptive learning-based solutions.

The authors Sarkar N. I. and Gul S. (2023) provided a review covering over 100 papers on AI-based autonomous UAV networks, focusing on planning, routing,

resource management, and energy efficiency. They emphasized the need to optimize these elements through ML with direct application to complex aquatic scenarios.

Recent studies on the action of drones on river courses, such as in *"Synergistic Reinforcement and Imitation Learning for Vision-driven Autonomous Flight of UAV Along River*" (Wang, Li, and Mahmoudian 2024) state that combining RL with imitation learning (IL) allows UAVs to navigate autonomously along rivers, relying on artificial vision, with a higher learning speed and increased accuracy. It also suggests a synergistic method that combines imitation learning and reinforcement learning for UAV navigation and obstacle avoidance in riverine environments. It addresses difficulties in partially observable, non-Markovian settings and improves performance and convergence rates by using a trainable simulation environment.

The authors Haris Malik and Hou Jin (2020, 1-22) present an actual problem, namely obstacle detection and safe navigation, this time of unmanned ground vehicles (UGVs), in situations where they have to follow a pre-established route. On the route that the vehicle had to follow, dangerous obstacles were mounted, which would have endangered the device. For the good implementation of artificial intelligence that makes efficient decisions based on the obstacles encountered, aspects regarding the distance, size, crowding, shape, and angle of the steering wheel were analyzed, intending to improve the navigation skills of the autonomous vehicles. This paper has applicability in the chosen topic, as obstacles represent a critical factor that the drone's AI must detect and avoid.

Moving on to the aerial realm, the authors Antonopoulos A., Lagoudakis M.G., and Partsinevelos P. (2022, 1-23) describe the development and deployment of an integrated UAV navigation system that provides real-time localization using optical, depth, and inertial data as well as the Global Navigation Satellite System (GNSS). To facilitate seamless integration into various systems and unfamiliar environments, the implemented system is built on top of a Robotic Operating System (ROS) environment package.

The Hierarchical Deep Q-Network (H-DQN), a solution based on hierarchical deep reinforcement learning, is used in a Semi-Markov Decision Process (SMDP) context (Qin, et al. 2022, 1-15). The Quality of Services (QoS) and energy security can be balanced with this technique. Additionally, it adjusts well to changing conditions using a variety of sensors and requirements. The concept applies to UAS-IoT with minimal power supplies, autonomous drone operations in areas with limited infrastructure, and environmental monitoring.

An algorithm for UAV navigation and obstacle avoidance in flood scenarios is covered in another paper that focuses on deep reinforcement learning (DRL) and its application to UAVs (Garg and Jha 2024, 1-12). This algorithm allows multiple UAVs to be controlled autonomously in order to collect obstacle data and determine safe routes for waterborne evacuation vehicles.

In the paper *"Neural network model for autonomous navigation of a water drone"* (Chekmezov and Molchanov 2024, 4-16), a neural network model for autonomous navigation of a water drone in a simulated fluvial environment is presented. Reinforcement learning is used to improve obstacle avoidance and water current adaptation, guaranteeing efficient navigation in dynamic conditions. Going further towards the subject of UAV simulation, it comes to studies that focus on software-in-the-loop simulation for testing vision algorithms with a quad-rotor UAV, utilizing Gazebo for simulation and PX4 for flight control (Nguyen and Nguyen 2019, 429-432; Nguyen Nguyen, and Ha 2019, 615-627). These aspects can also be utilized for further simulation within this article.

UAV security is another important factor that should not be overlooked. Another paper implements a three-class machine learning model on a UAV using a Raspberry Pi processor to classify GPS spoofing attacks in real-time, using GPS-specific features for effective detection and classification in location-dependent applications (Nayfeh et al. 2023, 289-292). With the use of a convolution neural network (CNN) feature extractor and machine learning classifiers, a study presents a low-cost Raspberry Pi 4-based system that uses ML for UAS detection and classification, attaining 100% accuracy in two-class detection and 90.9% in UAS type classification (Swinney and Woods 2022, 14). Furthermore, the paper "Autonomous *Control with Vision and Deep Learning: A Raspberry Pi Edge Computing Platform for Obstacle Detection in SUAV Path*" (Ullah, et al. 2024, 1-9) shows that this feature can be used for obstacle detection in Small Unmanned Aerial Vehicles (SUAVs) deployed on a Raspberry Pi. This setup enhances navigation safety through real-time obstacle avoidance in complex environments. In terms of security, for active countermeasures, C-UAS (anti-drone systems) can be used, which are a basic requirement for ground forces to be able to operate on the modern battlefield (Watling and Bronk 2024).

To sum up this subchapter, with a focus on energy efficiency, real-time adaptation, and security, the reviewed literature reveals a strong research focus on applying machine learning – specifically, deep neural networks, reinforcement learning, and imitation learning – to improve UAV autonomy, navigation, obstacle avoidance, data collection, and communication in challenging and dynamic aquatic or hostile environments. Also, one major issue that has been noted is the necessity of giving careful consideration to the credibility and dependability of machine learning in UAV operations and applications (Kurunathan et al. 2024, 1-28).

2. Methodology

2.1. The framework

The study is based on research into the concept behind implementing artificial intelligence in quadcopter devices that will be able to respond to user requirements, in different amphibious environments, and for various purposes. To understand the concept behind improving UAS control, the initial objective was to find answers to

several questions:

- What must the drone system contain to be capable of machine learning?
- What type of machine learning can be used?
- What parameters must be taken into account when used in unfriendly environments?
- What applications can be used to subsequently simulate these networks' frames?
- How can machine learning algorithms be integrated to allow UAVs to adapt in real time to uncertain conditions in river environments, in military situations?

The paper uses qualitative research methods, as, based on the analysis of the specialized literature and the created syntheses, new answers are sought to the previously formulated research questions, the objective of the research being the generation of new theoretical knowledge and the establishment of a conceptual framework for the implementation of artificial intelligence in unmanned aerial systems.
The data collection method was represented by documentary analysis, by collecting data and extracting essential information from different sources, in order to see the trends and research directions of various authors in the field. Thematic analysis was used as the qualitative analysis method.

This approach was chosen to highlight information of interest regarding the chosen topic, as well as to establish the basis for future research, which would include simulations and practical methods using real devices. The contribution leads to the systematization of aspects related to UAV control, which makes it possible to more easily simulate UAS in a virtual environment, respecting critical parameters. After simulating them in the virtual space, one can move on to the practical programming of a real device by "injecting" artificial intelligence to reduce the gap between the user's requirements and the device's intelligent sensors.

Limitations of the study include the lack of physical equipment for simulation and direct testing, thus leading to the lack of practical experiments, which are necessary to validate the results in a virtual and then a real environment.

2.1. Conceptual basis

Analyzing the specialized literature of the authors, it can be seen that they converge towards common principles and approve the need to improve some elements of UAS, but there are too few discussions about a single conceptual framework that would unify all these elements of UAS to obtain a viable and efficient solution in the area of aerial drone systems. Such a framework can be used with the ROS system, which is built to provide a modular approach for robotic applications. The individual development of functional blocks can be very useful, especially when designing highly complex applications. This approach allows for simple development, since each block has a very specific task (Antonopoulos, et al. 2022, 5).

Thus, based on the modular model of ROS and with the observations of other authors regarding some modules that should be developed, such as the ML inference engine (Foehn, et al. 2022, 2), the battery monitoring module (Barrientos, et al. 2011, 13) and the surveillance module (Queralta, et al. 2020, 11), in order to enable the intelligent and autonomous operation of UAVs in aquatic environments, a modular architecture is proposed that supports multi-agent coordination, real-time decision-making and autonomy based on ML. A similar modular architecture has been developed, but for search and rescue (SAR) operations (Queralta, et al. 2020, 1-2). The contribution of the present work is based on this validated approach, but adapted to the challenges of aquatic, riverine environments, with an emphasis on the ML-based decision module.

The architecture includes both on-board and edge-level components, combining sensor fusion, ML inference, control logic, and inter-agent communication, where data collected by sensors are processed locally (on-board), and decisions regarding flight, landing, or mission handover are made autonomously with the support of an ML module. This modular UAV-vessel approach was chosen because it allows the integration of critical functions, such as sensors, control, power, communications, and ML, in a scalable and robust framework, capable of responding to the specificities of fluvial environments. It is also justified by recent literature showing that modularity and distributed processing enhance the autonomy and resilience of UAS in multi-agent coordination (Antonopoulos, et al. 2022; Foehn, et al. 2022; Jung, et al. 2024).
Within this architecture, there will be two subsystems: the UAV and the central river vessel. The two subsystems are interconnected by a communication link (C2) and, in fact, constitute the overall unmanned aerial drone (UAS) system. Each subsystem is characterized by several specific modules (Figure 2), as follows:

The sensor module (GPS, IMU – Inertial Measurement Unit, barometer, on-board cameras) ensures the localization and perception of the surrounding environment, being the foundation of sensor fusion processes (Du, et al. 2020). The collected data are then processed by an ML inference module, which evaluates operational states (e.g., proximity to the vessel, battery level, landing safety, etc.). The role of this module is justified in the work of Foehn, et al. (2022), who demonstrate that running ML models directly on the UAV has rapid implications at the level of reaction in dynamic environments.

In order for algorithm-level decisions to be translated into precise movements, the architecture must include a flight control module. This connects the ML or RL algorithms to the autopilot system, using ROS 2 or PX4 (Nguyen and Nguyen 2019), thus translating intelligent behaviors into executable commands. Autonomy monitoring is ensured by a battery module, a necessary component for energy management and critical decision-making, an essential element in the structure of an intelligent UAS. Also, data exchange with other UAVs and the central vessel, in line with the inter-agent coordination concepts presented by Queralta, et al. (2020),

would be achieved using a communications module, closing the architecture at the UAV level.

As for the central vessel/ship, it is practically a control station, and the subsystem includes a UAV surveillance module, responsible for monitoring the active drones and triggering handover procedures, launching a new UAV when one returns for loading or fails, thus ensuring mission continuity. This functionality is similar to the drone swarm coordination strategies researched by Jung, et al. (2024, 7).
The difference between the two subsystems is that while the UAV platform has the ML module to make very fast decisions related to maintaining position, avoiding collisions, adjusting altitude, etc.

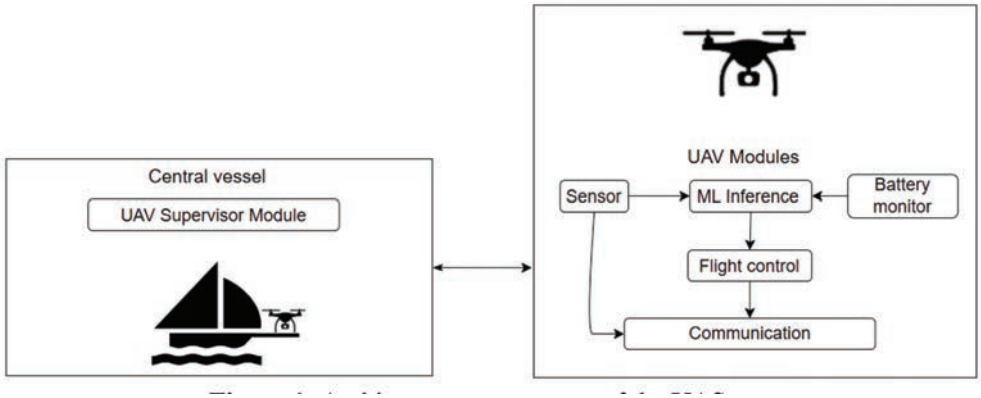

Figure 2 Architecture components of the UAS

The operational workflow, based on the diagram above, involves the UAV continuously sensing the position, altitude, and battery level, while the ML Inference Engine determines if the UAV is in a safe operational state. If a critical state is detected, the drone executes an autonomous landing on the fluvial vessel, whereas the supervisor module of the vessel triggers the launch of a standby UAV to continue the mission. This architecture can be implemented in ROS 2 with PX4 (MathWorks n.d.) and simulated in Gazebo using realistic riverine and aerial dynamics data.

The table below represents a light RL design focused on rewards (Guo, et al. 2023; Kong et al. 2023; Tovarnov and Bykov 2022) to better understand the reinforcement learning-based UAV control with perimeter maintenance in a fluvial environment (Table no. 1).

TABLE NO. 1

Light RL design on UAV control

State (S)	Action (A)	Reward (R)
While distance < 10 m to vessel & battery > 30%	Maintain position	+5
Distance between 10 m and 15 m	Adjust position	+1
Distance > 15m	Return towards the vessel	0
Battery < 20%	Land on the vessel's platform	+5 / -5
Collision	Any or N/A	-10

This approach introduces autonomy that adapts to real-time environmental changes (Table no. 2), including river current dynamics and narrow corridors, without the need for fixed, rule-based thresholds.

TABLE NO. 2

Light RL design based on environmental changes

State (S)	Action (A)	Reward (R)
Wind speed < 5m/s	Maintain normal flight	+3
Wind speed between 5m/s and 10 m/s	Adjust heading/thrust	+1 / -1
Wind speed > 10m/s	Initiate emergency landing	+ 5 / - 5
Visibility < 100m	Reduce speed, activate extra sensors	+3
Temperature between -10℃ and 40℃	Adjust battery saving mode/land	-3
Humidity > 90%	Enable sensor protection mode	+1 / -3

3. Results and discussion

3.1. Analysis of the theoretical and conceptual framework

Analyzing the specialized literature, as well as the previously proposed framework, the following answers to the research questions posed in Chapter 2 are found:
First of all, to allow the integration of machine learning, a drone must present an architecture similar to the one described, which combines both hardware and software elements. The components/modules were described in the previous chapter. Regarding the type of ML that can be used, taking into account the nature of the aquatic environment, characterized by variability and uncertainty, the most suitable type of machine learning is reinforcement learning (RL. This allows UAS to learn through interaction with the environment, adapting to new situations and optimizing decisions based on reward or penalty points, the goal being to maximize the score obtained. In more complex applications, more complex variants of ML, such as Deep Q-Network or hybrid learning, can also be used.

To answer the third research question, the parameters that need to be considered in hostile aquatic environments include atmospheric conditions (wind speed and direction, atmospheric pressure), hydrological conditions (water currents, water level, turbulence generated by obstacles), as well as static and dynamic obstacles (bridges, bank vegetation, other boats). Internal technical parameters, such as battery level, communication signal stability, and GPS positioning accuracy, are also determinants for mission success. Integrating this data through sensor fusion and using it in ML algorithms allows UAS to make robust decisions and reduce vulnerability to hostile conditions.

Aerial drone systems in river environments can be validated and tested within applications such as ROS 2 integrated with PX4, which allows for modular development of UAV components. A gazebo can also be used for simulations in

which environmental factors can be modified to reflect obstacles and adverse weather conditions specific to the river environment. These types of applications increase the realism and practical value of research involving drone systems in general.

Last but not least, to integrate ML algorithms into this drone technology, it is necessary to implement artificial intelligence at the UAV device level, through the presented architecture, but also at the level of the entire system, including the control station or center. The UAV, through a lightweight ML model, becomes capable of micro-decisions that must be taken in a very short time, while the system, through the control station and the data collection center, must be capable of the macro-decision perspective, having the overall situation of all drones in the field simultaneously, as well as the ever-updating Common Operational Picture (COP) (Figure 3). A combined use of all unmanned platforms would lead to an operationally efficient multi-domain system that provides a more complete common operational picture, due to its presence in the three environments – land, air, and sea. Each platform has its own areas that can be developed, many aspects being common, as can be seen in the compendium produced within the UNIDIR framework (Grand-Clément 2023, 12-16).

Figure 3 Common Operational Picture (COP) using aerial drone systems
Source: https://www.magaero.com/wp-content/uploads/2023/02/KINETIC-STRIKE-TRAINING-PROGRAM-KSTP-Image-1643901249160-RT.jpg

Aquatic environments and watercourses (rivers, canals, estuaries) present a series of particularities in terms of their influence on unmanned aerial platforms. They are distinguished by narrow spaces, variable dynamic conditions, and the short distance to the shore. Water currents, through their speed and direction, have an impact on ships that are landing platforms for drones; this requires the UAV to constantly calculate its position and trajectory. Approaching the shore practically implies the possible proximity to obstacles or objects that may represent obstacles, whether it is man-made infrastructure or vegetation specific to the site. The infrastructure can also represent a source of electromagnetic interference that disrupts the quality of communications between the UAV platform and the control station.

By integrating ML and artificial intelligence in general, drone systems can learn to react optimally to currents, based on previously simulated scenarios and stored in their unit. They can also make decisions in real time based on AI, detecting and avoiding obstacles autonomously, without human intervention. This ensures resilience for both the civilian and military sectors by anticipating risks and reducing reaction times across the entire drone system, which can include an increased number of such mobile aerial platforms.

3.2. Results on autonomous control of UAV in riverine environment based on rewards

A distance of up to 10 meters from the vessel is considered safe, as long as the battery is over 30%. This being the variant that the UAV must learn to obey, it will be scored the most, and the drone will have to maintain its position. If the distance increases, through the flight control module, the drone will have to adjust its position and will be scored only one point. If the distance exceeds the maximum value of 15 meters, then it is outside the aerial perimeter established for the vessel. In this case, the UAV must return to the designated area. If the battery drops below 20%, which is a critical level since the battery autonomy of drones is not great, it must land on the vessel's platform simultaneously with the second UAV that is on standby and which now has to activate and fly, replacing the one with the low battery. If the first drone lands successfully, it will be scored +5 points. If it fails to land properly or in a timely manner, it receives a score of -5. Ultimately, in the case of a collision between drones or with the environment, a penalty of -10 points was applied.

This entire concept automatically teaches technological systems through reinforcement learning to behave according to the highest score, modeling it by the characteristics set by the human mind. However, atmospheric conditions cannot be ignored in this regard. Each UAV has specific sensors to measure environmental parameters (e.g., an anemometer for wind speed, barometric sensors for atmospheric pressure, GPS for real-time localization, and LiDAR for obstacles). The data are used in ML algorithms to adapt the flight according to the real conditions, because it affects both the UAV dynamics model and autonomous decisions (e.g., landing when the wind is too strong). The learning process can also benefit from simulated failure cases in which UAVs deviate from optimal behavior. Penalizing these scenarios helps the agent learn robust fallback strategies more quickly. Although the simulation was based on idealized physics, future work should include validation with real telemetry data from UAV flights in aquatic environments to ensure the fidelity of the learned behavior.

It is important that both external environmental factors (e.g., air currents, vegetation, etc.) and internal conditions of UAV systems (battery level, stability of communication links, etc.) be within a unified risk assessment framework, as shown in a research article in the field of safety and security (Terje 2007, 745–754). The machine learning-based drone model should not only focus on optimizing navigation, but also on continuously assessing the risks and vulnerabilities specific

to the environment in which it operates, so that it is resilient, safe, and accurate.
From an operational perspective, the proposed architecture and the use of reinforcement learning directly contribute to the Military Decision-Making Process (MDMP), as can be easily seen below (Table 3). Thus, it is observed that UAS can operate on the MDMP principle or can be used in the decision-making process by military personnel.

TABLE NO. 3

The correlation between the military decision-making process and the modular UAS architecture

No.	Stage	Correlation
1	Receipt of Mission	UAVs can be quickly integrated into a specific mission, understanding and adapting to the requirements received from the higher echelon, including time, space, and resource constraints.
2	Mission Analysis	Integrated sensors and ML modules provide essential data about the environment (water currents, natural obstacles, weather conditions), facilitating the identification of critical tasks and the anticipation of risks in the operating space. Essential for the S2 compartment when UAS provides information.
3	Course of Action – COA Development	By using RL and prediction algorithms, UAVs can generate multiple courses of action (shortest or personalized path, maintaining the perimeter, landing on the ship, handover between drones), which can be adapted in real time. Also, courses of action established by the echelon can be implemented directly in UAS.
4	COA Analysis	ML-based simulations allow testing and evaluation of each course of action in complex river conditions, identifying strengths, vulnerabilities, and potential risks before implementation.
5	COA Comparison	Data resulting from previous assessments can be compared with each other, within several courses of action, providing the commander with an objective picture of the optimal solution. If this stage is integrated into the UAV subsystem, then it will be able to choose the best possible option.
6	COA Approval	Through UAS, synthesized data and recommendations can be transmitted, facilitating the selection process of the most viable course of action to the commander.
7	Orders Production	The integration of UAVs into a coordinated and robust network allows the translation of the approved decision into an executable operational plan, where each drone receives clear roles, synchronized with the overall mission.

3.3. Future work

Having the data on the aspects that need to be considered regarding the control of a drone through ML, the author can move on to the next step, which involves the hardware implementation of a physical drone capable of ML. Such a UAV device is built modularly, starting from a physical frame, such as those in the figures below (Figures 3 and 4), on which standardized electronic hardware is mounted.

This system is controlled by an open-source flight controller (e.g., Pixhawk), which runs firmware such as PX4 or ArduPilot, some of the most advanced and popular software systems for autonomous drones. This flight controller makes use of information from the PX4 repository to improve ArduPilot UAV mission safety and operational effectiveness (Tovarnov and Bykov 2022). The platform can be built manually, with components also available separately. After assembling the

Figure 3 F450 Quadrotor Drone
(Source: https://www.jsumo.com/f450-droneunassembled-4337-15-K.jpg)

Figure 4 QAV250 Quadrotor Drone
(Source: https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcQ5J_RzkS0IFLSAmAWAFVVrQ1P5YIDShJKriQ&s)

parts, connecting the motors, electronics, and sensors, and mounting them on the platform, it can be configured at the software level with applications such as QGroundControl (QGC).

This device is capable of executing multiple and various commands: autonomous flight, maintaining the perimeter, event detection, immediate and automatic reactions, automatic landing, handover between drones, etc. Furthermore, this UAV type is suitable for virtual simulations, using applications such as Gazebo and AirSim, where environmental parameters can be applied. Being open-source it means that the system has full control over the communication firmware, presenting compatibility with single-board computers (SBC) such as Raspberry Pi or Jetson. It presents a considerable advantage when it comes to low cost and accessibility, as well as its popularity. Implementing artificial intelligence based on machine learning and configuring the aspects presented above could make drones much more efficient and usable in agriculture, optimizing the time of activities in precision agriculture (Petre, et al. 2022, 105). As for the disadvantages, perhaps the biggest one is the low battery autonomy and the physical protection, which can yet be improved by utilizing additional protections for the platform's case. Due to technological limitations of batteries, drones cannot carry an additional or increased payload, as this disrupts their accuracy (Boşcoianu, et al. 2024, 12). Also, battery limitations are the cause of the major problem among drones, regardless of the field in which they operate, being one of the weaknesses of these technologies, which are still at the beginning of their development (Iagăru, et al. 2023, 296).

Future work will involve using real, low-cost, ML-capable physical drones and analyzing their behavior while they are being subjected to the experiment in amphibious environments and being programmed according to the requirements presented in this paper.

Conclusions

Integrating machine learning techniques into UAS control presents promising opportunities for improving autonomous operations in complex aquatic environments, such as rivers and streams. These environments pose unique

challenges, including water currents, variable weather conditions, and spatial constraints caused by vegetation and infrastructure.

Within the modular architecture, both the military decision-making process and the possibility of automatic learning based on rewards and penalties can be integrated at the AI module level. Through this ML-based UAS control, inter-agent coordination between UAVs is achieved, characterized by the transmission of data both to the central platform (ship) and to a field data collection center, thus making it possible to create and consolidate the common operational picture in real time and in a continuous, updated manner, based on the handover process between drones. This process supports the success of ISR (Intelligence, Surveillance, Reconnaissance), search and rescue, and military support operations. Also, through these handover mechanisms and battery monitoring, the energy management of UAS can be ensured, making it possible to extend the operational duration without direct human intervention, reducing logistical costs and risks for military personnel involved in the actions.

ML-based control strategies enable UAVs to adapt to such uncertainties in real time by learning robust flight behaviors, coordinated multi-agent navigation, and context-aware decision-making. Key insights include the development of adaptive algorithms for maintaining formation and position relative to moving platforms, reliable autonomous landing on ships in fluctuating water conditions, and seamless handover protocols to extend mission duration. Furthermore, the integration of real-time environmental sensors into ML models improves their resilience to atmospheric disturbances and hydrological variability.

The research questions were fully answered by defining the UAS architecture and selecting appropriate ML types. The specific parameters of the hostile river environment were identified, as presented in the table. Some specific applications of virtual simulations have been mentioned that can be used to validate the perspective of integrating UAS with ML and their use in adverse conditions, based on environmental factors that can be easily modified within these simulations. However, to be able to integrate UAS with ML, an AI module is needed, separately, at the level of the UAV itself, as well as at the system level, more precisely at the level of the control station and the data collection center, so that the perspective offered by the system is a complete one. However, the research questions are limited to a more theoretical level due to the lack of equipment and the actual simulation of the presented modular architectural framework.
Future research should focus on improving simulation environments that accurately model aquatic dynamics, combined with UAV behavior, expanding the datasets for training ML controllers in various scenarios, and validating the approaches through implementations in real conditions.

By harnessing the potential of ML, unmanned aerial systems can achieve a higher level of autonomy, safety, and efficiency, opening up new applications in environmental

monitoring, search and rescue, and inspection of aquatic infrastructure in various fields, including the military. However, to use it in the military field, an additional research perspective should be developed on the development of standardized protocols that ensure reliable and low-latency communication between UAVs and river platforms, allowing coordinated behaviors and the integration of systems from different suppliers at an international level.

References

Antonopoulos, Antonis, Michail G. Lagoudakis, and Panagiotis Partsinevelos. 2022. "A ROS Multi-Tier UAV Localization Module Based on GNSS, Inertial and Visual-Depth Data." *Drones* 6(6): 135. https://doi.org/10.3390/drones6060135.

Barrientos, A., J. Colorado, J. del Cerro, A. Martínez, C. Rossi y D. Sanz. 20112011. "Aerial remote sensing in agriculture: A practical approach to monitoring energy and mission performance." *Sensors* 18(8): 2559. https://doi.org/10.1002/rob.20403.

Boșcoianu, Mircea, Sebastian Pop, Pompilica Iagăru, Lucian-Ionel Cioca, Romulus Iagăru, and Ioana Mădălina Petre. 2024. "An Innovative Management Framework for Smart Horticulture—The Integration of Hype Cycle Paradigm" *Drones* 8, no. 7: 291. https://doi.org/10.3390/drones8070291.

Chellapandi, V.P., Liang Yuan, Stanisław H. Żak, and Zhaojian Wang. 2023. "A Survey of Federated Learning for Connected and Automated Vehicles." In *2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC)*, 2485–92. Bilbao, Spain. https://doi.org/10.1109/ITSC57777.2023.10421974.

Chekmezov, H., and O. Molchanov. 2024. "Neural Network Model for Autonomous Navigation of a Water Drone." *Information, Computing and Intelligent Systems Journal*, no. 5: 4–16. https://doi.org/10.20535/2786-8729.5.2024.315700.

Du, H., W.Wang, C. Xu, R. Xiao, and C. Sun. 2020. "Real-Time Onboard 3D State Estimation of an Unmanned Aerial Vehicle in Multi-Environments Using Multi-Sensor Data Fusion". *Sensors* 20: 919. https://doi.org/10.3390/s20030919.

Foehn, P., E. Kaufmann, M. Gehrig, R. Ranftl, A. Dosovitskiy, V. Koltun, and D. Scaramuzza. 2022. "Agile autonomous drone flight using end-to-end deep reinforcement learning." Science Robotics, 7(66). https://www.science.org/doi/10.1126/scirobotics.abl6259.

Garg, Armaan, and Shashi Jha. 2024. "Multi-UAV Assisted Flood Navigation of Waterborne Vehicles Using Deep Reinforcement Learning." *Journal of Computing and Information Science in Engineering* 24: 1–12. https://doi.org/10.1115/1.4066025.

Grand-Clément, Sarah. 2023. "*Uncrewed Aerial, Ground, and Maritime Systems: A Compendium.*" Geneva: UNIDIR. https://doi.org/10.37559/CAAP/23/ERC/05.

Guo, Y., N. Zhang, H. Jiang, J. Li, and Q.-Y. Fan. 2023. "Layered Reinforcement Learning Design for Safe Flight Control of UAV in Urban Environments." 673–78. https://doi.org/10.1109/csis-iac60628.2023.10363849.

Haris, Malik, and Jin Hou. 2020. "Obstacle Detection and Safely Navigate the Autonomous Vehicle from Unexpected Obstacles on the Driving Lane." *Sensors* 20(17): 4719. https://doi.org/10.3390/s20174719.

Hassanalian, Mostafa, and Abdeslam Abdelkefi. 2017. "Classifications, Applications, and Design Challenges of Drones: A Review." *Progress in Aerospace Sciences* 91: 99–131. https://doi.org/10.1016/j.paerosci.2017.04.003.

Iagăru P., M. Boşcoianu, I.L. Cioca, I.M. Petre, S. Pop, F.A. Sârbu, and R. Iagăru. 2023. "Critical Analysis of Mini Unmanned Aerial Vehicles (UAV) Development Capabilities and Perspectives of Effective Integration in Horticultural Agroecosystems in Romania". Scientific Papers. Series "Management, Economic Engineering in Agriculture and Rural Development", Vol. 23 Issue 1, 293-302. ISSN 2284-7995. https://managementjournal.usamv.ro/pdf/vol.23_1/Art33.pdf.

Jung, Wooyong, Changmin Park, Seunghyeon Lee, and Hwangnam Kim. 2024. "Enhancing UAV Swarm Tactics with Edge AI: Adaptive Decision Making in Changing Environments." *Drones* 8(10): 582. https://doi.org/10.3390/drones8100582.

Khan, A., J. R. Campos, N. Ivaki, and H. Madeira. 2023. "A Machine Learning Driven Fault Tolerance Mechanism for UAVs' Flight Controller." 217–27. https://doi.org/10.1109/prdc59308.2023.00034.

Kong, S., M. Li, Y. Zhou, and Z. Wang. 2023. "Effective Control of Unmanned Aerial Vehicles Based on Reward Shaping." 135–39. https://doi.org/10.1109/rcae59706.2023.10398796.

Kurunathan, H., H. Huang, K. Li, W. Ni, and E. Hossain. 2024. "Machine Learning-Aided Operations and Communications of Unmanned Aerial Vehicles: A Contemporary Survey." *IEEE Communications Surveys and Tutorials* 1. https://doi.org/10.1109/comst.2023.3312221.

Maharjan, Narayan, Hiroaki Miyazaki, Bikash M. Pati, Matthew N. Dailey, Sudeep Shrestha, and Takayuki Nakamura. 2022. "Detection of River Plastic Using UAV Sensor Data and Deep Learning." *Remote Sensing* 14(13): 3049. https://doi.org/10.3390/rs14133049.

MathWorks. n.d. "Control a Simulated UAV Using ROS 2 and PX4 Bridge." Accessed July 20, 2025. https://www.mathworks.com/help/ros/ug/control-a-simulated-uav-using-ros2-and-px4-bridge.html.

Nayfeh, M., J. Price, M.A. Alkhatib, K. Al Shamaileh, N. Kaabouch, and V.K. Devabhakuni. 2023. "A Real-Time Machine Learning-Based GPS Spoofing Solution for Location-Dependent UAV Applications." 289–93. https://doi.org/10.1109/eit57321.2023.10187344.

Negru, Sorin A., Patrick Geragersian, Ivan Petrunin, and Weisi Guo. 2024. "Resilient Multi-Sensor UAV Navigation with a Hybrid Federated Fusion Architecture." *Sensors* 24 (3): 981. https://doi.org/10.3390/s24030981.

Nguyen, Kim D., and Toan-Tuan Nguyen. 2019. "Vision-Based Software-in-the-Loop-Simulation for Unmanned Aerial Vehicles Using Gazebo and PX4 Open Source." In *International Conference on System Science and Engineering*, 429–32. https://doi.org/10.1109/ICSSE.2019.8823322.

Nguyen, Kim D., Toan-Tuan Nguyen, and Chien Ha. 2019. "Graph-SLAM Based Hardware-in-the-Loop-Simulation for Unmanned Aerial Vehicles Using Gazebo and PX4 Open Source." In *Lecture Notes in Computer Science*, 615–27. Cham: Springer. https://doi.org/10.1007/978-3-030-26969-2_58.

Nomikos, Nikolaos, Panagiotis K. Gkonis, Panayiotis S. Bithas, and Panagiotis Trakadas. 2023. "A Survey on UAV-Aided Maritime Communications: Deployment Considerations, Applications, and Future Challenges." *IEEE Open Journal of the Communications Society* 4: 56–78. https://doi.org/10.1109/OJCOMS.2022.3225590.

Petre, Ioana, Mircea Boșcoianu, Sebastian Pop, Pompilica Iagăru, Flavius Aurelian Sârbu, and Romulus Iagăru. 2022. "An Analysis of the Possibilities to Develop and Implement a Modular and Scalable System Based on Mini-Aerial Robots for Precision Agriculture." RECENT - REzultatele CErcetărilor Noastre Tehnice. 23. 100-106. https://doi.org/10.31926/RECENT.2022.68.100.

Qin, Zhen, Xiaojie Zhang, Xinyu Zhang, Bin Lu, Zhiqiang Liu, and Lihua Guo. 2022. "The UAV Trajectory Optimization for Data Collection from Time-Constrained IoT Devices: A Hierarchical Deep Q-Network Approach." *Applied Sciences* 12 (5): 2546. https://doi.org/10.3390/app12052546.

Queralta, J.P., J. Taipalmaa, B.C. Pullinen, V.K., Sarker, T.N., Gia, H. Tenhunen, and T. Westerlund. 2020. "Collaborative Multi-Robot Search and Rescue: Planning, Coordination, Perception, and Active Vision." in *IEEE Access*, vol. 8, pp. 191617-191643. https://doi.org/10.1109/ACCESS.2020.3030190.

Samus, Mykhailo. 2024. "*Lessons Learned from the War in Ukraine: The Impact of Drones.*" Bucharest: New Strategy Center. https://newstrategycenter.ro/wp-content/uploads/2024/02/Lessons-Learned-from-the-War-in-Ukraine.-The-impact-of-Drones-2.pdf.

Sarkar, Nurul I., and Sonia Gul. 2023. "Artificial Intelligence-Based Autonomous UAV Networks: A Survey." *Drones* 7(5): 322. https://doi.org/10.3390/drones7050322.

Song, G.G. 2022. "A Deep Reinforcement Learning Strategy for UAV Autonomous Landing on a Platform." In the *2022 International Conference on Robotics and Smart Systems (ICRSS)*, 104–9. https://doi.org/10.1109/ICRSS57469.2022.00031.

Swinney, C.J., and J.C. Woods. 2022. "Low-Cost Raspberry-Pi-Based UAS Detection and Classification System Using Machine Learning." *Aerospace* 9(12): 738. https://doi.org/10.3390/aerospace9120738.

Terje A. 2007. "A unified framework for risk and vulnerability analysis covering both safety and security". Reliability Engineering & System Safety, Volume 92, Issue 6, Pages 745-754. ISSN 0951-8320. https://doi.org/10.1016/j.ress.2006.03.008.

Tovarnov, M.S., and N.V. Bykov. 2022. "Reinforcement Learning Reward Function in Unmanned Aerial Vehicle Control Tasks." *Journal of Physics: Conference Series* 2308 (1): 012004. https://doi.org/10.1088/1742-6596/2308/1/012004.

Ullah, F., M. Hayajneh, N. AbuAli, H. Asad, F.S. Malik, and B.F. Mon. 2024. "Autonomous Control with Vision and Deep Learning: A Raspberry Pi Edge Computing Platform for Obstacle Detection in SUAV Path." 1–9. https://doi.org/10.1109/commnet63022.2024.10793296.

Wang, Zhaojian, Jianwen Li, and Nina Mahmoudian. 2024. "Synergistic Reinforcement and Imitation Learning for Vision-Driven Autonomous Flight of UAV Along River." In *2024 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 9976–82. Abu Dhabi, United Arab Emirates. https://doi.org/10.1109/IROS58592.2024.10801487.

Watling, J. and Bronk, J., 2024. "*Protecting Land Forces from Uncrewed Aerial Systems (UAS)*", Wilson Center Canada. Canada. https://static.rusi.org/protecting-the-force-from-uncrewed-uas.pdf.

Wu, Lin, Chao Wang, Pengfei Zhang, and Chao Wei. 2022. "Deep Reinforcement Learning with Corrective Feedback for Autonomous UAV Landing on a Mobile Platform." *Drones* 6(9): 238. https://doi.org/10.3390/drones6090238.

Zhao, Chenjie, Ryan Wen Liu, Jingxiang Qu, and Ruobin Gao. 2024. "Deep Learning-Based Object Detection in Maritime Unmanned Aerial Vehicle Imagery: Review and Experimental Comparisons." *Engineering Applications of Artificial Intelligence* 128: 107513. https://doi.org/10.1016/j.engappai.2023.107513.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Development and Use of Drones in the Romanian Armed Forces: Current Trends and Operational Perspectives

Adrian HUȚAN*

*"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
e-mail: adrian.hutan97@yahoo.com

Abstract

This paper explores the integration of unmanned aerial vehicles (UAVs) in the Romanian Armed Forces, particularly focusing on the Bayraktar TB2 system. It evaluates the strategic and tactical impact of drones in modern warfare, especially in coordination with F-16 multirole fighter operations. Through the use of real-time intelligence, surveillance, and laser-guided systems, drones enhance operational capabilities such as target designation and precision strikes. The study references conflict examples like Nagorno-Karabakh and Ukraine to support operational perspectives. The conclusion emphasizes the necessity of a national UAV strategy for Romania aligned with NATO objectives.

Keywords:
Air-to-Ground Coordination; Drone Integration; F-16 Operations; Romania; UAV Strategy.

Article info
Received: 30 July 2025; Revised: 29 August 2025; Accepted: 9 September 2025; Available online: 6 October 2025

Citation: Huțan, A. 2025. "The Development and Use of Drones in the Romanian Armed Forces: Current Trends and Operational Perspectives." *Bulletin of "Carol I" National Defence University*, 14(3): 278-287. https://doi.org/10.53477/2284-9378-25-48

The rapid evolution of drone technologies is transforming modern military doctrines and national defense capabilities. Romania, as part of NATO, faces increasing security challenges along its eastern flank and has begun integrating unmanned aerial vehicles (UAVs) to enhance its operational flexibility.
The use of drones in modern warfare has proven indispensable for reconnaissance, target designation, and even direct engagement. In Romania's case, the acquisition of the Bayraktar TB2 UAVs from Turkey marks a critical step toward modernizing its defense systems. The increasing relevance of hybrid threats in the Black Sea region reinforces the urgency for integration, doctrine adjustment, and technological adaptation, as seen in Baykar Technologies (2023). *Bayraktar TB2 technical overview*.

This paper analyzes the current state and future perspectives of drone use in the Romanian Armed Forces in comparison with neighboring countries and allies, drawing lessons from regional conflicts and NATO doctrine. Emphasis is placed on practical deployment, interoperability, and doctrinal transformation.
The current security dynamics in the Black Sea region, particularly in the context of Russian aggression in Ukraine, demand increased ISR capabilities and airspace awareness. Romania, located on NATO's eastern flank, plays a critical role in regional deterrence and early warning missions.
Integrating UAVs into Romania's national defense architecture is not only a matter of technology adoption but also a doctrinal challenge. A cohesive national drone strategy must address not only procurement, but also operational procedures, personnel training, legal frameworks, and allied coordination. This study aims to contribute to that process by offering an evidence-based comparative assessment and highlighting doctrinal gaps that must be addressed.

Literature Review and Conceptual Framework

Modern literature on unmanned aerial vehicles focuses on their strategic role in shaping asymmetric warfare. Scholars such as P.W. Singer (2009) and Shlapak, D.A., & Johnson, M.W. (2016) have highlighted the way drones are transforming the modern battlefield, shifting the paradigm from traditional, manned systems to remote and autonomous warfare. Sources such as the International Institute for Strategic Studies (IISS 2023) and NATO Air Command (NATO 2022). distinguishes between different classes of drones—from small tactical UAVs to large, armed MALE (Medium Altitude Long Endurance) systems—and underscores their growing role in intelligence, surveillance, and reconnaissance (ISR), strike capabilities, and electronic warfare.

NATO defines UAVs as core components of its intelligence, surveillance, and reconnaissance (ISR) architecture, supporting both deterrence and strike functions as per Genini D. (2025). The Romanian Army Transformation Strategy 2040 echoes these values, emphasizing C4ISR modernization and autonomous capabilities as future pillars of national defense.

Case studies from the Nagorno-Karabakh war (2020), the war in Ukraine (2022–present), and Turkish drone operations in Syria serve as real-world evidence of how effective UAV integration can alter the operational balance of a conflict. These conflicts have demonstrated that low-cost, high-precision UAVs, when properly integrated into command-and-control systems, can replace or complement traditional airpower.
The growing global proliferation of UAVs also raises concerns related to arms control, export restrictions, and the ethical implications of autonomous and semi-autonomous systems. While NATO members focus on UAV integration into conventional force structures, other state and non-state actors increasingly deploy drones for asymmetric warfare.

Authors such as Anderson, D. (2018) and Friedman, G. (2019) argue that drone use without proper legal frameworks may undermine long-term stability and violate international humanitarian law. Therefore, conceptual discussions around the legitimacy of targeted strikes, airspace sovereignty, and civilian oversight are now part of most military academic analyses.

In Romania, the legal and ethical framework regarding drone use is still evolving, with current doctrinal references focusing more on interoperability than on the legal conditions for deployment in peacetime or under hybrid threats.
Romania's conceptual framework for drone integration remains in quite early stages, but includes references to NATO STANAGs, joint air-ground interoperability, and peacetime airspace regulation for UAV flights.

In NATO doctrine and Romanian military strategic documents, drones are acknowledged as vital tools for increasing situational awareness, operational flexibility, and rapid deployment capabilities. Their use supports principles of precision warfare and force protection. Theoretical approaches in contemporary security studies also underline the dual-use nature of drones, applicable in both combat and civil operations, necessitating careful regulation and strategic integration.

Materials and Methods

This paper employs a qualitative research approach based on:

- Documentary analysis of official military strategies, NATO doctrine, and defense reports;
- Comparative case study between Romania, Bulgaria, and Turkey.

Primary sources include the Romanian Ministry of National Defense (MApN 2023), NATO publications, and specialized defense journals. News coverage and press releases regarding acquisitions (e.g., Bayraktar TB2) also provide recent operational insight.

The criteria used in the comparative table below include:

- UAV platform types and origin;
- Operational use (ISR, strike, support);
- Level of domestic defense industry involvement;
- Readiness for combat deployment.

This method helps highlight Romania's positioning within the regional UAV capability spectrum. The study is limited by access to classified operational details and dynamic changes in acquisition policy.

In addition to operational criteria, the study also considers the degree of doctrinal integration of UAVs within NATO standards. This includes referencing relevant NATO STANAGs such as STANAG 4586 (UAV interoperability), STANAG 4609 (motion imagery), and STANAG 5516 (Link 16 communication protocol). These documents provide a framework for evaluating how well Romania's UAV capabilities align with alliance-level interoperability and command-and-control structures.

Although Romania has acquired modern UAV platforms, the lack of a national doctrine or fully institutionalized procedures for integrating drones into joint operations limits their strategic potential. Therefore, this methodological framework also considers doctrinal adaptability and the role of network-centric warfare capabilities in determining UAV readiness.

A critical limitation of this study lies in the classified nature of Romanian defense acquisitions and operational doctrine. While open-source materials, government statements, and press releases provide baseline data, there is a lack of transparency regarding training programs, software architecture, and joint mission planning frameworks. These aspects limit the ability to fully assess doctrinal maturity or compare real-world combat readiness between states.

Comparative Analysis: Romania, Bulgaria, Turkey

The table below summarizes the key dimensions of UAV integration in the selected countries:

TABLE NO. 1

UAV Capability Comparison – Romania, Bulgaria, Turkey

Country	UAV Platforms	Operational Use	Local Industry Involvement	Combat Readiness
Romania	Bayraktar TB2, Watchkeeper X	ISR, Target Designation	Partial (Elbit, Aerostar)	Medium
Bulgaria	Hermes 450 (planned), Orbiter	Border Surveillance	Minimal	Low
Turkey	Bayraktar TB2, Akıncı, Anka	ISR, Precision Strike, EW	Full domestic production	High

Interpretation:

- Turkey leads with an integrated UAV-industrial ecosystem;
- Romania shows operational progress but depends on external suppliers;
- Bulgaria remains behind in terms of operational deployment.

Romania's partial industrial capability (Elbit Systems and Aerostar) offers the potential for growth in domestic UAV maintenance, modification, and data-link adaptation — but doctrinal implementation remains at an early stage.
The ongoing war in Ukraine has served as a critical case study for drone effectiveness in modern warfare. In this context, Romania, Bulgaria, and Turkey offer contrasting examples of how UAV capabilities are developed and deployed.

Turkey has emerged as a global leader in drone technology, particularly through its Bayraktar TB2 systems. Turkish drones have played a decisive role in multiple conflicts (e.g., Libya, Nagorno-Karabakh, and Ukraine), establishing Turkey as a key drone exporter and innovator.

Bulgaria, on the other hand, has taken a more conservative approach, investing in surveillance drones but lacking combat-ready UAVs. Recent discussions in Sofia suggest a growing awareness of the need to accelerate drone integration, particularly for border security and NATO operations.

Romania has taken steps to modernize its forces by procuring TB2 drones from Turkey and exploring partnerships with NATO allies. However, its domestic production capabilities remain limited compared to those of Turkey. The proximity to the Ukrainian conflict has spurred faster integration of UAVs into Romanian defense strategy, with a focus on ISR and operational deterrence along its eastern border.

This comparative approach reveals Romania's intermediate position—more advanced than Bulgaria in UAV deployment, but still dependent on foreign suppliers, unlike Turkey. It is also worth noting that while Turkey achieves full-spectrum drone autonomy, Romania's current lack of payload integration capability and indigenous AI systems highlights the need for technological transfer partnerships or local development funding. Bulgaria, by contrast, has not operationalized any combat drone capability as of 2025.

Another significant dimension in comparing the three countries is their approach to defense-industrial development and sovereign production capacity.
Turkey's success stems from long-term investment in its defense ecosystem, with companies like Baykar, Aselsan, and Roketsan enabling full-cycle development — from airframes to EO sensors and munitions. In contrast, Romania relies primarily on foreign technology integration, with limited UAV production or R&D at the national level, despite capabilities at firms like Aerostar Bacău and Romaero.

Additionally, the absence of a consolidated governmental policy for drone-industry growth limits public-private partnerships and technology transfer. Regional cooperation projects, such as participation in PESCO (Permanent Structured Cooperation) or NATO DIANA (Defense Innovation Accelerator), remain underutilized.

Bulgaria's delays in procurement stem partially from procurement bureaucracy and a lack of industrial partners capable of sustaining even low-end ISR platforms. In contrast, Turkey has become not just a regional UAV power but a net exporter of strategic drone capability, changing the balance of influence in areas like Libya, Syria, and the Caucasus.

Results and discussions

Drones are altering the character of war at both the tactical and operational levels. The comparative analysis conducted in this paper highlights three key findings regarding UAV integration in the Romanian Armed Forces, as benchmarked against Turkey and Bulgaria.

A relevant case study that demonstrates the effectiveness of tactical drone employment is the war in Ukraine. During the early phases of the 2022 Russian invasion, Ukrainian forces made extensive use of Bayraktar TB2 UAVs to target supply convoys, command posts, and short-range air defense systems.

What proved most effective was not merely the UAV platform itself, but the flexibility of the Ukrainian doctrine, which allowed decentralized units to operate drones autonomously with real-time battlefield awareness. In contrast, more hierarchical and rigid structures — such as those employed by Russian forces — delayed adaptation and suffered greater losses.

This comparison reinforces the idea that Romania must not only acquire UAV platforms but also invest in doctrinal modernization, C2 integration, and decentralized mission planning to fully exploit the potential of its drone assets in future conflicts.

a) Strategic Positioning

Romania is currently positioned in the middle of the regional spectrum: it has made significant acquisitions (e.g., Bayraktar TB2 and Watchkeeper X), but lacks the fully integrated industrial ecosystem Turkey benefits from. Unlike Bulgaria, which is still in the planning phase with limited capability, Romania is operationalizing drones in ISR and targeting roles, albeit without indigenous production or autonomous doctrine.

b) Operational Use Cases and Joint Air Operations

UAVs are currently being used primarily for intelligence, surveillance, and reconnaissance (ISR), as well as target designation for strike missions. In a NATO context, drones are expected to support multirole fighters such as the F-16.

One of the major tactical advantages of UAV deployment is air-to-ground coordination. Bayraktar TB2 systems, for instance, can lase targets for fighter aircraft, providing real-time battlefield information without exposing pilots to ground-based air defenses. This technique, tested in Turkish operations in northern Syria, can be

replicated within the Romanian Air Force by integrating UAVs into command-and-control architecture and tactical data links (e.g., Link 16).

c) Operational Advantages of Drone–Fighter Coordination

Coordination between UAVs and fighter aircraft, especially in SEAD and CAS missions, enables layered strike capabilities. UAVs can identify and lase targets while F-16s engage from standoff ranges, minimizing pilot exposure and increasing mission efficiency. This tactic, as explained in the Romanian Air Force (2022), was successfully implemented in Turkish operations in Syria and can be adapted to Romanian air doctrine with appropriate data link and C2 integration.

d) Doctrinal and Technical Challenges

Despite the procurement of modern UAV platforms, Romania still lacks an institutionalized drone doctrine. There are no unified operational procedures for integrating UAVs in combined arms operations. Additionally, issues such as limited access to secure satellite communications (SATCOM), insufficient airspace regulation for autonomous systems, and a lack of trained drone operators hinder full operational capacity.

The data suggests that Romania must move beyond acquisition and focus on conceptual integration, local R&D, and NATO-compliant procedures to truly benefit from UAV capabilities.

Another important matter to consider is the ethical and regulatory framework in drone use. The use of drones raises critical ethical and legal questions, especially when employed in offensive operations. International Humanitarian Law (IHL) and the Geneva Conventions govern the use of force, and drones must comply with principles of distinction, proportionality, and necessity.

Romania, as a NATO and EU member, is bound by these norms and has developed military regulations regarding the lawful use of drones. Challenges include:

- Accountability for actions taken by autonomous or semi-autonomous systems;
- Protection of civilian populations in conflict zones;
- Transparency in rules of engagement;
- Cybersecurity and data privacy, particularly for surveillance operations.

The debate extends to the risk of over-reliance on drones, potentially lowering the political threshold for initiating military actions. These concerns demand robust regulatory frameworks, operator training, and public oversight.

Conclusions

The integration of drones in the Romanian Armed Forces represents more than a technological modernization — it is a strategic necessity in today's hybrid warfare environment. While Turkey demonstrates what a fully sovereign UAV doctrine and

industrial base can deliver, Romania remains at an intermediary stage: procuring performant platforms but relying heavily on foreign technology.
UAVs already enhance Romania's ISR capacity and target acquisition capabilities in support of the F-16 fleet. However, the full potential remains underexploited due to doctrinal delays, limited C2 (Command & Control) integration, and underdeveloped airspace regulations.

In the long term, Romania must not only adopt foreign UAV platforms but also work toward doctrinal and industrial independence. By investing in secure communication systems, indigenous UAV design, and NATO-standard mission planning tools, Romania can transform drones from tactical assets into strategic force multipliers.

Several key lessons emerge from Romania's experience and global trends, so the following actions could be considered:

- Diversify sources of UAV systems to avoid overdependence on single suppliers.
- Invest in domestic R&D to build a national drone ecosystem.
- Enhance training and integration of UAVs into multi-domain operations.
- Develop ethical and legal guidelines aligned with NATO and EU frameworks.
- Given Romania's geostrategic position, a compelling proposal would be the creation of a NATO Drone Hub in the Black Sea region. This hub could:
- Support joint training and interoperability among NATO forces;
- Facilitate drone testing and innovation;
- Serve as a regional command center for ISR missions.

A National Drone Strategy should also be established, outlining clear procurement, innovation, and operational goals for the next 10–15 years, ensuring Romania remains a credible actor in the age of autonomous warfare.
Drones are altering the character of war at both the tactical and operational levels. The traditional battlefield is increasingly populated by autonomous and semi-autonomous systems, requiring adaptations in military doctrine and force structure.

Studies such as those made by NATO (2020) show that drones contribute to:

- Increased battlefield transparency and real-time decision-making;
- New forms of hybrid warfare, blending conventional and irregular tactics;
- Force dispersion and mobility, allowing smaller units to operate independently with air support;
- Operational tempo acceleration, reducing the time between target detection and engagement.

Having introduced new forms of asymmetry in military confrontations, the NATO scene must take into consideration the fact that even non-state actors can now acquire or build drones, challenging the traditional dominance of state militaries, as shown by Biddle, S. (2021).

Other case studies illustrate this:
In Ukraine, drones have enabled smaller units to destroy armored vehicles and command posts at a fraction of the cost of traditional weapons.
In Nagorno-Karabakh, Azerbaijani drones overwhelmed Armenian defenses, proving that air superiority can be achieved without manned aircraft, also stated by Gibbons-Neff, T. (2020) and Bronk, J., & Gady, F.S. (2021)
These examples demonstrate how drones shift the power balance by lowering entry barriers to high-impact operations. For Romania, this means developing both offensive and defensive drone strategies to protect critical infrastructure and deter aggression, especially near the Black Sea.

The integration of drones into the Romanian Armed Forces is not just a technical modernization but a strategic necessity. While Romania has made commendable progress, continued effort is needed to fully leverage UAVs in both national defense and NATO operations. Through balanced investments in technology, regulation, and doctrine, and by capitalizing on regional partnerships, Romania can ensure that it remains resilient and agile in the face of 21st-century security threats.

ACKNOWLEDGEMENTS
The author expresses his sincere gratitude to Associate Professor, Ph.D. NATE Silviu, for his valuable guidance and continuous support in the preparation of this academic paper.
Special thanks also go to the teaching staff of the „Nicolae Bălcescu" Land Forces Academy and to the publicly available resources provided by the Romanian Ministry of National Defense and NATO doctrine centers.

References

Anderson, D. 2018. *The future of warfare: Modern conflict and military strategy*. Oxford University Press.

Baykar Technologies. 2023. *Bayraktar TB2 technical overview*.

Biddle, S. 2021. *Military power: Explaining victory and defeat in modern battle*. Princeton University Press.

Bronk, J., N. Reynolds, and J. Watling. 2021. "The air and missile war in Nagorno-Karabakh: Lessons for NATO." RUSI Occasional Paper. https://static.rusi.org/special-report-air-and-missile-warfare-nagorno-karabakh.pdf

Friedman, G. 2019. "The World in 2019: A Year on the Edge." *Geopolitical Futures*. https://geopoliticalfutures.com/world-2019-year-edge/

Gibbons-Neff, T. 2020. "Azerbaijan's drone campaign in Nagorno-Karabakh." *The Washington Post*. https://www.washingtonpost.com/world/europe/nagorno-karabkah-drones-azerbaijan-aremenia/2020/11/11/441bcbd2-193d-11eb-8bda-814ca56e138b_story.html

Genini, D. 2025. "Countering Hybrid Threats: How NATO must adapt after the War in Ukraine." *Journal of Strategic Studies.* https://journals.sagepub.com/doi/full/10.1177/09670106241284172

International Institute for Strategic Studies (IISS). 2023. *The military balance 2023*. Routledge.

Ministry of National Defense (MApN). 2023. *Romanian armed forces transformation strategy 2040*. https://mapn.ro

NATO. 2020. "NATO 2030: United for a new era." https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf

___. 2022. "Modern air power and the role of ISR assets in Eastern Europe." https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/241007-hybrid-threats-and-hybrid-warfare.pdf

Romanian Air Force. 2022. "F-16 Fighting Falcon în serviciul României." *Revista Forțelor Aeriene* (2): 15-29. https://roaf.ro

Scales, R.H. 1999. "Future Warfare. U.S. US Army War College Press." https://press.armywarcollege.edu/monographs/154

Shlapak, D.A., and M.W. Johnson. 2016. "Reinforcing Deterrence on NATO's Eastern Flank: Wargaming the Defense of the Baltics." https://www.rand.org/pubs/research_reports/RR1253.html

Singer, P.W. 2009. *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin Press.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Responsible Warfare. US-Iran Case

Iulian CHIFU, PhD*
Cosmin GRIGORE, PhD Candidate**

*Professor, "Carol I" National Defence University;
President, Conflict Prevention and Early Warning Center, Bucharest, Romania.
e-mail: keafuyul@gmail.com
**National School of Political and Administrative Studies (SNSPA);
Junior Researcher at the Center for Conflict Prevention and Early Warning, Bucharest, Romania.
e-mail: grigore.cosmin@yahoo.com

Abstract

In the conundrum of legality, legitimacy, and morality regarding war and war operations, the concept of responsible warfare could find its place. The operational definition of such a concept or even behavior has its place somewhere between the legitimate and moral sides, since an ethical component is present in the idea of responsible warfare, not only in the legitimate access to force and use of military power, but also in the legal component associated with it. In this article, we aim to identify specific pieces of concrete behaviour in times of war that would substantiate this concept and could be a basis for responsible behavior. Our major test case is the recent attack by the US on Iranian nuclear facilities and the counter-reaction from the regime of Ayatollahs to retaliate proportionally and avoid escalation. The link between promoting a responsible warfare and the effectiveness of reaching the objectives in war could be, however, instrumental to challenge as well as advocating to any extention of such a practice.

Keywords:
Responsible Warfare; Legal; Legitimate; Moral Actions in War; Military Retaliation; Escalation.

Article info
Received: 14 August 2025; Revised: 2 September 2025; Accepted: 12 September 2025; Available online: 6 October 2025

Citation: Chifu, I., and C. Grigore. 2025. "Responsible Warfare. US-Iran Case." *Bulletin of "Carol I" National Defence University*, 14(3): 288-306. https://doi.org/10.53477/2284-9378-25-49

Introduction and Methodology

The article aims to identify the nuances between legal, legitimate, and moral in terms of warfare operations, and the place of a concept of responsible war/warfare in this conundrum. Moreover, through a heuristic approach, we are aiming at identifying behaviour that could fit into the understanding of a responsible war definition and could lead us to promote it, when taking into consideration the big struggle between means and ends, costs and benefits in times of war, all related to the effectiveness of chivalrous behaviour in war times.

We have done an encyclopaedic assessment of the domains, criteria, indicators, and schools of thinking related to legal, legitimate, and moral approaches towards the war, in general. This would indicate the real place of responsible war as a concept and the need and place of such a concept, as well as the epistemological use of such a concept. After establishing the content and operational definition based of the previous studies about responsibility in war and previous attempts to create such a perspective, we are making a poli-heuristic study on concrete cases of behaviour involving responsibility in war that would show us that the concept has a concrete practical part and consequences that need to be explored so that this concept could be welcomed in the theory related to war.

Responsible warfare involves legal, legitimate, and moral components of military action.

1. Legality and war

The war changed dramatically in form, shape and participants (Chifu and Simons 2023), and the mix in the space of hybrid components, and full spectrum warfare (Chifu and Grigore 2025) has altered also the understanding of the war and the legislation about the way of conducting wars, criminal acts in war, civilians, and their involvement and responsibilities in wartimes. We have covered a big part of the conundrum about legality, legitimacy, and morality in war (Chifu 2024c) that could stay in the fundamentals of our debate here. We have identified that the boundaries between war and peace nowadays are very blurred. The relativization of war and combat and the hybridization of confrontations (Chifu and Simons 2023) require an increasing number of criteria to decipher ambiguities and interpretations.

First, the most important part of the legal debate comes from the distinction between civilians and militaries, and then about the distinction between combatants and non-combatants. The debate about proportionality in war came naturally since war no longer justifies the excessive number of civilian casualties (Chifu 2024b). Armies do not fight against civilians, so the killing of civilians is generally prohibited during war according to the laws of war. The Geneva Conventions' fundamental provision is not to directly target civilians who are not participating in the war (United Nations 1949).

But real operations come with side effects, unintentionality, collateral damage, and civilian victims, even if we have planning and clear rules of engagement, minimizing the civilian victims, when fighting in crowded areas or where military targets are hidden or embedded in civilian communities.

Discussing responsible warfare leads us also to look at the theory of a just war: A war is considered just, right, only if the good it brings outweighs the bad it causes on that occasion (Hurka 2005). An effect of war achieved by unfair methods or exceeding the expected benefits of the operation can lead to responsibilities (Fabre 2009). Here we can include, of course, the legal grounds for military intervention, ranging from self-defense to combating terrorism, genocide, nuclear non-proliferation, and the responsibility to protect, all UN grounds for legitimate intervention (Simons şi Chifu 2017).

The legal basis for intervention, the grounds set out in the UN Charter, and the previous conventions on combating terrorism, nuclear non-proliferation, and genocide are clear (United Nations 2001; 1951; 1968). In the humanitarian law, the 2005 resolution on the responsibility to protect (R2P) (United Nations 2005), respectively the 2005 World Summit document (A/RES/60/1) and the 2007 letter from the UN Secretary-General to the President of the Security Council (S/2007/721), which highlighted the need to operationalize the principle of the responsibility to protect (United Nations 2007) could be less clearer and acceptable, but making the way to legitimacy of war. Security Council resolution on Libya (United Nations 2011a; 2011b) may serve as validation at the UN level of this principle and associated provisions (Chifu 2011). The relationship between the responsibility to protect and the equal national sovereignty of UN member states, and the right to interfere on the territory of a member state of the organization (Glanville 2014) is still to be settled legally.

2. Legitimacy and war

The objectives of the war could require, when planning, the necessity of the action that creates side effects on civilians, but the legitimacy of such a step should include that the actions taken against civilians do not constitute punitive acts, but ones strictly related to the logic and planning of the war (Fabre 2009). In the criteria and indicators related to legitimacy, we could include the number of casualties of combatants and civilians compared with the objectives and achievements, when there's a legitimate military strategy of the party concerned (Fabre 2015). The expressed desire and consecutive actions taken to end the war are part of the legitimacy, as well as attempts to avoid sliding towards wars of attrition (May 2012).

The debate on proportionality in war also includes efforts to stop and end the war (Chifu 2024c), which constitutes a basis for legitimacy. The link between the just or unjust nature of a war and the conclusion of a just or unjust war is made through two principles clearly derived from the legal component of the law of

war: a belligerent waging a just war may be obliged to fight to end the war before fully achieving the objectives of its just war; on the other hand, a belligerent who has entered into an unjust war may obtain legal justification for continuing the war based on the behaviour and observance of the rules of war by its counterpart (Chifu 2024c). Hence, the importance of constantly seeking ways to end the war, but also of ensuring the legitimacy and legality of continuing it until its conclusion, even if the initial objectives have not been achieved.

We found references to criteria related to legitimacy at war linked to a legitimate authority to declare the war, as well as the ultimate goal of a just peace, pursued from the beginning of the conflict (Christopher 2004). The criteria for assessing whether it is right, fair, and just (from a legal point of view) to engage in combat would also be fivefold: the seriousness of the threat justifying the use of military action; the motivation or primary objective of the military action; the last option: if there are no reasonable peaceful alternatives available; the proportionality of the military response (particularly in terms of the number of casualties and destruction); the balance of consequences (the result brings more good than pain and costs through the intervention carried out) (Contratto 2012).

Here is also the place to discuss the difference between exiting a war and ending a war. Exiting a war has rarely been done through peace agreements/treaties, at least since 1994 (Chifu and Voicu 2015). Ending a war is still determined by clear, legally binding documents. But even if legal documents or guarantees are present, there are numerous cases when the war re-emerges in the same conditions – see the Budapest memorandum 1994 for Ukraine (CSCE 1994), ignored 20 years later by the annexation of Crimea, and the Chechen peace Treaty 1996, broken three years after (UN Peacemaker 1996) with a new devastating war. That underlines the limits of the legitimacy criteria in war times, since legitimacy enshrines also the sustainable respect for existing engagements – *bona fides* (Kotzur 2009) – or respect in good faith of the signed international documents.

So, the legitimacy component refers to refraining from and avoiding launching an attack that could incidentally result in the loss of civilian lives, injury to civilians, and destruction of civilian objects that would be excessive in relation to the anticipated direct military advantage (ICRC 1977, art.57, para.2). Legitimacy requires that the criterion of just cause be balanced by those of last resort, the immunity of non-combatants, and the principle of proportionality.

3. Morality and war ethics

We are not going to make a full theory of morality and war. Professional armies today increasingly rely on civilians as a source of combatants and military resources, weapons, and components that can only be used in war, a situation which, from the point of view of legitimacy, qualifies them to assume responsibility in war and forfeit the general rights of civilians in war (Fabre 2009).

There are two big schools of thinking: the one based on the theory of just war and discrimination against non-combatant civilians that are claiming, however, the due responsibility of civilians, and the one that rejects such distinction and considers that the immunity of non-combatants must be absolute according to the humanitarian law, claiming that the profound morality of war is what defines and governs these principles, which are not found in the laws of war (Shue 2008); (Roberts 2008). The same with the issue of global/national responsibility (Nuremberg type) or of global indiscriminate sanctions for all citizens or groups and communities versus distributive justice – judging each one according to its own direct acts – which is deeply controversial in the case of war and civilian responsibility (Cohen 2008; Miller 2008; Williams 1998; Kymlicka 2002).

The same tensions come when assessing what's proportional and what's disproportionate, predictable but unintended in terms of killing and injuring non-combatants (Lango 2014), with high moral ground claiming a larger impunity for such military to civilian attacks and larger immunity for civilians and non-combatants, and a lot of caveats, limitations and extra rules at any point, from planning to execution, in the case of professional armies. Not talking about other operations when parts of morality and war ethics would interdict in full operations like political assassination, the right to legally kill in revenge, the punishment of treason, and repression, which we've studied (Chifu 2024a). The same applies to using nuclear rhetoric in any context, the nuclear rhetoric, or even the possible use of nuclear weapons (Chifu 2023).

Cases of the use of responsible actions in times of war

The responsible actions are rated in the niche between legitimate and moral behaviour, even though critics from the human rights organisations often debate this issue. It refers to actions that avoid secondary loss of life at the expense of the effectiveness of the military operation. It involves both warning about and abstaining from military action, or creating conditions for limiting the human secondary casualties, both civilian and military. In this space, we've discovered and studied three types of classical conventional actions in military operations: roof knocking, phone calls, and leaflets, as well as the use of loudspeakers. It is true that, in some cases, those warnings had a side effect on psychological operations that can't be denied. However, they are worth mentioning and studying since they represent a good step forward in the right direction, using them to avoid human casualties in war.

1. Roof knocking

This is a characteristic of the IDF, the Israeli Army, and refers to a military strategy created in 2009 by the Israeli Air Force to alert the Gazan population to evacuate structures it had identified as housing Hamas's command posts, rocket caches, or ammunition storage facilities. It has subsequently been applied in a number of conflicts (Magramo, et al. 2023). Before a major hit is carried out, IDF soldiers will

drop a tiny, non-explosive munition on the top of a building to warn the occupants that the building is the target of an airstrike (Withnall 2014). By permitting evacuation in structures where militant organizations store rockets or munitions, it seeks to reduce the number of civilian casualties (Lister and Abdelaziz 2014). The attack came some 15 minutes after the warning.

However, human rights organizations have challenged this contentious approach (Magramo, et al. 2023). First, because there were errors of judgment recorded. Second, because in such a heavily populated neighborhood, the damage of missiles cannot be limited to a single house – see the attack on a building near al Batsj mosque struck by shrapnel, or individuals that stayed too close to a building that has been targeted for attack, being hit by flying metal, wood, and concrete. UN estimates that 70% of those hits are civilians (Magramo, et al. 2023).

"There is no way that firing a missile at a civilian home can constitute an effective 'warning'", stated Philip Luther of Amnesty International, in condemnation of the so-called 'knock on the roof' tactic (Withnall 2014). Another criticism is that despite the warning, there aren't many secure locations for civilians to find in a blockaded area. Moreover, in the recent Gaza war, Israel appears to have given up on the "knock on the roof". IDF spokesperson Lt. Col. Richard Hecht stated on October 11, 2023, that "Hamas didn't knock on the roof when they entered and threw explosives at our ambulances. It's war. It's a different scale", with reference to the October 7 attacks (Magramo, et al. 2023).

2. Phone calls and leaflets

Phone calls and leaflets were used in multiple cases by the IDF and the American Army. Both the 2008-09 and 2012 Israeli-Palestinian conflicts in Gaza made use of leaflets and phone messaging. They were partially an attempt to clear areas where Israeli troops planned to concentrate strikes, and they were partially political in nature, accusing Hamas of causing the violence. Leaflets cautioning people not to approach the border within 300 meters were distributed during both battles. Leaflets alerted locals in 2012 that terrorist groups were lurking among them and posed a direct threat to their safety. An IDF report states that around 2.5 million leaflets were distributed in 2008–09. About 165,000 phone messages sent the same message (Lister and Abdelaziz 2014). The Israeli military has also used radio and television broadcasts to broadcast warnings during previous operations against Hamas.

In the case of the American Army, in the 2003 Iraq campaign, leaflets dropped from US planes were asking villagers in southern Iraq to tune into radio stations run by "Coalition forces". Hundreds of thousands of leaflets warning soldiers to stay away from damaged installations that are likely to be hit again have also been sent to them. Messages were specific - "repairing the facilities puts Iraqi military lives at risk and that the Coalition has targeted fiber optic cables for destruction"; "To ensure your safety, avoid areas occupied by military personnel"; "targeting Coalition aircraft or

tracking them with radar could result in Coalition air strikes" – or part of a psyops campaign - "Coalition forces do not wish to harm the noble people of Iraq"; "The Coalition does not wish to destroy your landmarks" - were dropped also to civilian or to Iraqi air defense forces (Moss 2003).

3. The use of loudspeakers

For sure, in all those cases, critics are referring to psyops rather than warning or responsible warfare aimed at avoiding casualties. But one cannot ignore that perspective, the fact that the side effect is, however, spearing civilian lives. It is true, on the other hand, that in some cases it is very difficult to separate those two objectives. Moreover, when it is about the use of loudspeakers, it's impossible not to consider that the first aim is psychological operations, even though the secondary one can mean a responsible warfare behaviour. The use of psychological operations during the Second Gulf War also led to minor successes, when 20 Fedayeen fighters in Nasiriyah were persuaded to surrender by mobile PsyOps teams in Humvees equipped with loudspeakers. In some cases, they were used for promoting revolt (Taylor 2007).

Responsible war concept. An operational definition

Taking on from the previous cases, we've conducted an encyclopaedic research in the literature about the roots of a responsible war concept that would be needed in the evolution of just war theory, situated between legitimate and moral action in the triad legal-legitimate-moral (Chifu 2024c). We traced responsibility concerns at the level of debates about the first use of a nuclear weapon in Hiroshima and Nagasaki, in fighting insurgency wars, in the campaign in Kosovo and NATO's commitment to zero casualties, but specially now, in the modern age, discussing drones, cyber attacks and the conventional military reaction to them, the use of automated weapons system and the a.i. driven decision-making in lethal weapons use.

The Declaration of St. Petersburg of 1868 proclaimed that the only legitimate object of war was to weaken the military forces of the enemy and that, for this purpose, it was sufficient to disable the greatest possible number of men (ICRC 1868). The Geneva Protocol I of 1977 introduces the duty, before carrying out an attack, to "do everything feasible to verify that the objectives to be attacked are (...) military objectives" (ICRC 1977, art.57, para 2(a)(i)). Feasible precautions may be defined as those which are "practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations". The Conventional Weapons Convention of 1981 contains similar language in the Amended Mines Protocol of 1 May 1996, Art. 3, para. 10 (ICRC 1996).

The documents, mandatory for the signatories, also introduce the rule of doubt: in case of doubt whether a person is a civilian or whether an object is normally dedicated to civilian purposes, the Protocol lays down a presumption of civilian status

(ICRC 1977, Art.50, para1; Art.52, para.3). The political and military planners of the NATO air campaign in the Kosovo conflict of 1999 were determined that it should be carried out strictly in accordance with the law of armed conflict. "The targets were exclusively military — every effort was made to avoid collateral damage — planes only fire at targets when we are confident that we can strike accurately — some aircraft in the first operation returned without dropping ordnance. Targets are carefully selected and continuously assessed to avoid collateral damage" (Shea 1999). Even in this case, there were, inevitably, some instances of collateral damage, as it was on 14 April 1999, an attack on what was defined as the lead vehicle of a column of military vehicles, which proved to be a refugee column near Djakovica (Rogers 2000).

Responsible warfare is also linked to the legitimacy of the use of military force and individuation of responsibilities in such operations in order to justify the use of military force. This is also linked to the use of force involved in military detention or targeted killing (Issacharoff and Pildes 2013). This also needs a greater judicial role in assessing wartime judgements and separating the state of war and the rules associated with it, and the judgements and guarantees for accused individuals in peacetime. These changes are not yet directly reflected in the formal laws of war, but are important in the legitimate and moral debate. As is the very idea of eliminating through direct action and killing of a direct enemy, commander, or political decision-making in times of war or peace (Chifu 2024a).

1. Guerrilla warfare and civilian casualties

Guerrilla warfare, in which fighters merge with the civilian population, tends to increase civilian casualties. In post-1945 conflicts, guerrillas prefer to launch attacks out of civilian anonymity at the enemy's weak points, often using tactics such as ambush very successfully. The situation is exacerbated when guerrillas, partisans, freedom fighters, or other armed factions are engaged in combat in towns or populated areas (Trooboff 1975). The result of these trends has been an increase in civilian casualties in armed conflicts: according to the Swiss Federal Office for Civilian Protection, the ratio of the First World War was 200 military: 1 civilian; in the Second World War, nearly 1:1, and in the Vietnam War, 1 military: 20 civilians (Sassoli and Bouvier 1999).

The big clash is, however, between the need for effectiveness in war operations, the ambition of military commanders not to expose militaries to unnecessary risks, and the need to avoid secondary unnecessary casualties, especially civilians (Nafziger 1976). Reducing military casualties to a minimum and maintaining the public support for a war are also very important in an era with "the CNN effect", a reference to the embedded television reporters with the troops, in the Iraq war, and the media reports, often broadcast at the same time as events unfold in a campaign. But even more so nowadays, when anybody with a cell phone could become a reporter and reference to any event in the field.

A full debate is launched regarding weak states and responsibilities for the attacks coming from their territories. It refers to Afghanistan and the 9.11 attacks, but also to the threat to a neighbouring state coming from a separatist regime or an irregular actor out of the reach and control of the sovereign state (see debates about threats coming from separatist Transnistria from the Republic of Moldova and Russia's war of aggression in Ukraine) (Chifu 2022). Sovereign states have a responsibility not only to protect their own citizens but also to protect the rights and fundamental security interests of other states within their own territory (Deng, et al. 1996). However, many states around the world lack the resources to do so. The problem is not always the state's inability but rather its unwillingness to prevent irregular activity on its territory (Reinold 2011).

Safe havens have been defined as "ungoverned, under-governed, or ill-governed areas of a country where terrorists … can organize, plan, raise funds, communicate, recruit, train, and operate in relative security because of inadequate governance capacity, political will, or both." (US Department of State 2009) The responsibility for the conduct of irregular forces who use their territory as a launching pad for attacks against other states is a debate about attribution that challenges the restrictive standard that prevailed in international law, which largely absolved states with irregular forces in their territories from responsibility and military responses for acts of those autonomous actors. The global fight against terrorism, however, has strengthened the notion of responsibility even in those cases.

2. Cyber war and legitimate self-defense

In the case of cyber-attacks, two are the most important issues, related to the relevance of ethics to cyberwarfare, assessed by George Lucas in a case-based approach involving the Russian distributed denial of service (DDoS) attack against Estonia for the latter's relocation of a Russian war memorial (2007), the Stuxnet attack on Iranian centrifuges, likely perpetuated by a collaboration of United States and Israeli intelligence (2010), the Guardians of the Peace – likely a North Korean group – hack of Sony Pictures, apparently in protest of Sony's then-soon-to-be-released *The Interview*, a parody assassination attempt of Kim Jong-il (2014) and the Chinese data breach of the Office of Personnel Management (OPM), which compromised over 21 million employee records (2015) (Lucas 2017).

The number and diversity of those cases allow covering a wide range of responsible warfare operations, aiming at identifying cyberattacks against civilian or military targets, but also involvement in democratic internal processes like the Russian meddling in the United States' presidential election (2016). But the most important part of the debate is *casus belli*: when does a cyberattack legitimize the self-defense with conventional means, meaning the use of force? Could a cyber attack be considered an armed attack? (Balendra 2008; Ruys 2010)

Responsible warfare is prompted by legitimate and clear arguments in legal terms, but also a suitable, robust self-defense that maintains the support of the population for

the government and the military. Here, the commensurability problem, meaning the dimension of the harm, is at stake in order to decide the proportionality that could refer to a kinetic attack as a reply. A big debate also refers to the physical damages (Stuxnet) and human casualties created after a cyber attack. Lucas sticks to the idea that the need for reaction comes only if a cyber attack causes physical damage to people or objects in the real world. In some other cases, Singer and Friedman consider the need for "sufficiently serious" consequences to open the door to retaliatory kinetic response against a non-kinetic attack (Singer and Friedman 2013).

We could also have a grave attack on the financial sector, or supplies of essential goods and services, by blocking state internet, inaccessible sites, bank disturbances, elections, attacks non physical that are, however, more damaging on rules and freedoms of numerous individuals and, therefore, could make the case for a kinetic attack in response (Fritz, Henschke and Strawser 2016). The debate comes down to figuring out the magnitude of the least harm that would activate the right to self-defense for settling the threshold for a conventional response.

3. Automated warfare, drones, a.i.

Maybe the most prominent debates related to responsible warfare are coming from the new technologies and their use in wartime. And for a reason, once they change the full spectrum of rules, and since the current legislation doesn't cover this blooming evolution of technology and its implications in the military operations or associated. In all those cases, the most important principle for responsible warfare is that someone must be held responsible for all actions taken in a military conflict (Sparrow 2007). But how could this responsibility play a role in the cases of automated systems, a.i., or the use of autonomous drones?

What Champagne and Tonkens call the responsibility gap (Champagne and Tonkens 2015) is about someone filling a "blank check" for the actions of autonomous robotic devices, a person of sufficiently high standing that could accept responsibility even if that person could not be causally linked to those actions besides this prior agreement. Occupying a decision posture in an office could come, though, with the responsibility involving personal freedom and wealth for the deeds of an automated system under the person's surveillance. Matthias has dubbed "the responsibility gap" (Matthias 2004) since one's freedoms could not be linked to an unpredictable future guided by technical choice.

Robots cannot make decisions on the basis of their own initiative, but rather on preprogrammed commands. But military weaponry is somehow capable of making programmed choices and decisions in ways that are unpredictable and not in line with pursuing that end in a morally acceptable manner. The full debate is very extensive (Asaro 2008; Krishnan 2009; (Singer 2010) and engages themes like how the responsibility in warfare could be engaged? "If there are recognizable war crimes, there must be recognizable criminals." It is natural to want to carry this principle

over to automated warfare (Walzer 1977). Arkin suggested "a responsibility advisor" that autonomous lethal robotic systems will be equipped with, which "makes explicit to the robot's commander the responsibilities and choices she is confronted with when deploying autonomous systems capable of lethality" (Arkin 2009).

Autonomous weapon systems could erode humans' decision-making power or alter their decisions when doing face recognition or suggesting targets, even though the human decides and acts by issuing the order to shut down a human target. The situation could be complicated once such weapons have been deployed, and humans will not be able to change or abort their targets. Although autonomous weapons have significant decision-making power, currently, they are not able to make ethical choices. As Robillard and Persons are assessing, in order for Just War Theory to be fully adequate, it must both recognize the unique set of battlefield harms caused by structures as well as account for them by means of a notion of structural responsibility (Robillard 2011). Ethical implications of AI integration in the military decision-making process and how the characteristics of AI systems with machine learning (ML) capabilities (Nalin and Tripodi 2023) might interact with human decision-making protocols are at stake. It's up to the humans to assess a machine's ethics and employ it in its specific and limited sector when built for a particular purpose, like a tracking and triage system designed for disaster relief operations (Etzioni and Etzioni 2017).

Sauer and Schornig are concerned about the nexus between democracy and the military use of unmanned systems, the drones. The debate is about the democratic distinctiveness: the ways in which democracies are distinct from other regime types. Democratic Peace Theory does not make space for that distinction in the use of drones for surveillance, and they support the idea that such use of armed and eventually autonomous systems could thwart democracies in the long run and render themselves only more war-prone and even slide toward authoritarian regimes (Sauer and Schörnig 2012).

Effectiveness constitutes the other reference in responsible warfare, related to the protection of life and minimum risk for soldiers. Machines can operate in hazardous environments; they require no minimum hygienic standards; they do not need training; and they can be sent from the factory straight to the frontline. There are numerous advantages to the military, especially in relation to dangerous tasks. They are used in dangerous situations such as forward reconnaissance, bomb disposal, or the suppression of enemy air defences, being exposed to the enemy in the first place, before humans are. We need to use them. Therefore, the complexity of the debate about responsible warfare.

Operational definition

Based on previous debates about responsible warfare and the applied cases underlined above, we have extracted the characteristics necessary and have presented

the following definition of responsible warfare/war (we prefer to go deeper than war for obvious reasons, since a number of debated activities are rather in the hybrid and non-military part of the defense and security).

Responsible warfare is a behaviour and conduct of warfare operations that is designed to prove restrain and avoid escalation of any kind, aims at minimum or zero human casualties and no harm to human life or way of life, even though that behaviour has to sacrifice efficiency, but not the safety of soldiers or raising the risk of man in uniform, not talking about civilians.
That type of activity is different from legal, legitimate, moral approach to war and warfare operations since responsible warfare/war should be legal, in the context of existing legislation, should be legitimate, in order to maintain the support of the public and should aim at maintaining a high moral ground if possible, even though conflicts of value could distort the ideal responsible behaviour from a purely moral one. The balance between effectiveness and no harm should always privilege the second, and any breach of the (moral) rules should have a very clear argument in the realm of the effort to achieve the aims of the operation and, at the same time, avoid victims and costs of any kind.

The US-Iran case: avoiding nuclear catastrophe, due retaliation, and terminating a military confrontation

The case that we are proposing to discuss in the framework of responsible warfare is the attack of the US on the nuclear sites of Iran on the 22nd of June 2025, and the consecutive attack of Iran on the al-Udeid American military base in Kuwait two days later (Chifu 2025a). The case is consecutive to Israel's 12-day bombing attack on the nuclear facilities, command and control, leadership, and experts on nuclear military issues developed beginning with the 13th of June 2025, which cleared the way for the American intervention with bunker-buster bombs (we do not discuss here Israeli operations). The United States attacked the Iranian nuclear sites, destroying them irrevocably, according to a statement to the nation made by US President Donald Trump (The White House 2025a).

In the case of the US, it was a unique intervention, with aircraft taking off from the United States and returning to their bases in the US, without any intermediate landings in the Middle East, without a declaration of war, and with the clear objective of preventing Iran from acquiring nuclear weapons. The original Israeli attack began on June 13, the night after the International Atomic Energy Agency, the UN institution responsible for supervising and monitoring the nuclear area, issued a very clear and harsh report (IAEA 2025) stating that Iran was not complying with the JCPOA (Department of State 2015) – which remains in force for the three European states and the organization, even though the US has withdrawn from the agreement. The reason: blocking the inspectors' access to monitoring facilities, avoiding or silencing the communication of activities related to the nuclear program

with the claim of being civilian, and hiding military nuclear facilities revealed by Israeli and American intelligence services.

In all, Iran breached both the nuclear non-proliferation rules and its own commitment in the JCPOA. There are claims that military nuclear use of enriched Uranium for a bomb is not an option, especially since the fatwa issued in October 2003 by the Supreme Leader Khamenei is active and forbids Muslims from producing nuclear weapons (Sirjani 2013). But it is a weak argument in the debate since the enrichment at 60% and more could never be explained by medical, energy supply, or research needs. There is a discussion about responsible warfare linked to preemptive strikes, as we have to consider also if that attack could happen under Article 51 of the Charter on self-defense, or would have needed a Security Council resolution. But that's rather a juridical and political debate.

Israel was able to destroy only the group of scientists responsible for the nuclear program, the military leadership, and the Islamic Revolutionary Guard Corps, and the accessible surface or shallow nuclear sites, along with Iranian air defenses and missile production. Israel "knew in advance" the strikes would not destroy the uranium (I24 News 2025). So the United States had to intervene to prevent the destruction of deeply buried nuclear sites. The result was the destruction of this program, with a grand part of the nuclear product covered deep *in situ*, under some hundred tons of debris, and some of it being extrait in advance from those sites in order to avoid that the bombing could risk a nuclear contamination: Israeli Prime Minister Benjamin Netanyahu told Israeli media on August 12 that Iran still holds about 400 kilograms of enriched uranium, though Iran may still be unable to access this stockpile (I24 News 2025), a quantity consistent with the International Atomic Energy Agency (IAEA)'s estimate in June 2025 that Iran retained about 408.6 kilograms of 60 percent enriched uranium (Borens, et al. 2025), less than what is needed for a nuclear weapon. Mario Grossi confirmed repeatedly that no radiation or incident was associated with those military operations (Newsonair 2025).

The goal of destroying the Iranian nuclear program was achieved (The White House 2025b; 2025c), as the attack has hit some 3 to 6 hours after the warning was launched by the US forces, enough time for the Iranians to retreat the personnel and nuclear-enriched uranium, but not being able to extract all its centrifuges and other elements of technological nuclear facilities. Prime Minister Benjamin Netanyahu stated that Israel continues to monitor Iran's nuclear weapons program in coordination with the United States and will act with or without US approval (I24 News 2025). Iranian President Masoud Pezeshkian acknowledged on August 10 that Israeli strikes had damaged nuclear capabilities and warned that rebuilding them could prompt further attacks (Borens, et al. 2025).

As a reply, Iran launched 13 missiles against the US military base, but also after a warning that allowed the movement of the aircraft and personnel from the

base (Seddon and Pomeroy 2025). As in the case of Iran, the level of destruction was enormous, but no casualties; in the case of the US, only one missile reached the target. Both parties achieved their aim; the US destroyed the nuclear facilities, and Iran formally retaliated by hitting the US base in the Gulf. Both avoided any escalation, as well as significant human casualties, as the US avoided any secondary nuclear crisis (Chifu 2025b).

The responsible warfare definition applies here, in spite of the more debatable issues related to the legality of the strike – the Security Council approval versus interpretation of self-defense, non-proliferation versus preemptive strike, JCPOA broken agreement, and US military intervention. And it goes both ways: the US avoided Iranian casualties in the nuclear direct operation, as Iran avoided American ones. It proved restrained, observance of a plan designed to avoid escalation or human casualties.

How definitive is this intervention? How quickly will Iran rebuild its nuclear military program? These are issues that bring us into the realm of eternal war and the imposition of peace by force, with the ultimate objective of leading to a just and lasting peace. All are debatable in the framework of responsible warfare through the long-term consequences of a military operation. But the first layer of any analysis will consider that exchange of actions as being an example of a responsible war.

Conclusion

Is this exchange of US and Iran military intervention, observing the perspectives of avoiding escalation and human casualties, going to create a trend? It is difficult to know at this point. But the needs of both power politics, self-defense, and public support for military operations could lead to those behaviours being reproduced, and even could lead to a trend in legitimate interventionism with a huge regard for the consequences and respect of ethics, in a responsible warfare.

References

Arkin, R.C. 2009. *Governing lethal behavior in autonomous robots.* Boca Raton: Chapman and Hall.

Asaro, P.M. 2008. "How just could a robot war be?" In *Current issues in computing and philosophy*, by A. Briggle, K. Waelbers and P. Brey (Eds.), pp. 50–64. Amsterdam: Ios Press.

Balendra, Natasha T. 2008. "Defining Armed Conflict." *Cardoza Law Review* 29 (6): 2461–2516. https://ssrn.com/abstract=1022481.

Borens, Avery, Andie Parry, Ben Rezaei, Katherine Wells, Carolyn Moorman, Adham Fattah, Kelly Campa, and Brian Carter. 2025. *Iran Update.* https://understandingwar.org/research/middle-east/iran-update-august-13-2025/.

Champagne, Marc, and Ryan Tonkens. 2015. „Bridging the Responsibility Gap in Automated Warfare." *Philos. Technol.* 28: 125–137. doi:10.1007/s13347-013-0138-3.

Chifu, Iulian. 2011. „Libia şi operaţiunile NATO. Reîntoarcerea de la voluntarism la regulile clasice ale dreptului internaţional." *Impact Strategic* 2 (39): 116-127. https://cssas.unap.ro/ro/pdf_publicatii/is39.pdf.

___. 2022. *Ameninţări şi conflicte în secolul 21.* Volumul 2 din tetralogia Reconfigurarea securităţii şi a Relaţiilor Internaţionale în Secolul 21. Bucureşti: Editura RAO.

___. 2023. „Disaster, attack, or nuclear accident caused by Russia: scenarios, probability, and consequences." In *Medical Response Strategy in Case of Radiation Emergency Caused by the War in Ukraine*, by Florin-Catalin Cirstoiu, Victor Juc, Corina Silvia Pop, Petre Min and Cristian Barna. NATO Science for Peace and Security Series, Springer.

___. 2024a. „De la James Bond la asasinatul politic: Relativizarea etică a dreptului de a ucide legal ca răzbunare, sancţionarea trădării şi represiune. Cazul Ismail Hanyieh la Teheran." *Infosfera* (nr. 4): 11-21.

___. 2024b. „Delicatul balans al proporţionalităţii în Gaza: până unde merge dreptul la autoapărare şi când e genocid." *Adevărul.* https://adevarul.ro/blogurile-adevarul/delicatul-balans-al-proportionalitatii-in-gaza-2335134.html.

___. 2024c. „Lege, etică şi legitimitate vizând proporţionalitatea în război. Cazul Gaza." *Infosfera* (nr. 1): 5-19. https://www.mapn.ro/publicatii_militare/arhiva_infosfera/documente/2024/1_2024.pdf.

___. 2025a. *Pacea cu forţa şi războiul etern. Cazul Iranului.* https://www.caleaeuropeana.ro/iulian-chifu-pacea-cu-forta-si-razboiul-etern-cazul-iranului/.

___. 2025b. *Război în Orientul Mijlociu. Israel şi distrugerea sistematică a programului nuclear iranian.* https://www.caleaeuropeana.ro/iulian-chifu-razboi-in-orientul-mijlociu-israel-si-distrugerea-sistematica-a-programului-nuclear-iranian/.

Chifu, Iulian, and Alexandru Voicu. 2015. *Reconstrucţie post-conflict.* ISBN 978-606-609-909-7. Bucureşti: Editura Rao.

Chifu, Iulian, and Cosmin Grigore. 2025. "Război cu spectru larg. De la extinderea instrumentelor la a gândi inimaginabilul." *Gândirea Militară Românească* (nr. 2): 10-35. doi:10.55535/GMR.2025.2.01.

Chifu, Iulian, and Greg Simons. 2023. *Rethinking warfare in the 21-st Century. The influence and effects of the Politics, Information and Communication Mix.* Cambridge University Press.

Christopher, Paul. 2004. *Ethics of War & Peace.* 3rd ed. Pearson Prentice Hall.

Cohen, G.A. 2008. *Rescuing Justice and Equality.* Cambridge, MA: Harvard University Press.

Contratto, Michael R. 2012. *The Decline of the Military Ethos and Profession of Arms: An Argument against Autonomous Lethal Engagements.* Air University Press. www.jstor.com/stable/resrep13670.

CSCE. 1994. "Budapest Document 1994. Towards a New Partnership in a New Era." https://www.osce.org/files/f/documents/5/1/39554.pdf.

Deng, Francis M., Sadikiel Kimaro, Terrence Lyons, Donald Rothchild, and William I. Zartman. 1996. *Soveregnty as Responsibility. Conflict Management in Africa.* Brookings Institution Press. https://www.jstor.org/stable/10.7864/j.ctv80cc8b.

Department of State. 2015. *Joint Comprehensive Plan of Action.* https://2009-2017.state.gov/documents/organization/245317.pdf.

Dinstein, Yoram. 2001. *War, Aggression and Self-Defence.* 3rd ed. Cambridge: Cambridge University Press.

Etzioni, Amitai, and Oren Etzioni. 2017. "Incorporating Ethics into Artificial Intelligence." *Journal of Ethics* 21 (4). doi:10.1007/s10892-017-9252-2.

Fabre, Cecile. 2009. "Guns, Food, and Liability to Attack in War." *Ethics* (The University of Chicago Press) 120 (1): 36-63. https://www.jstor.org/stable/10.1086/649218.

___. 2015. "War exit." *Ethics* 125 (3): 631-652. https://www.jstor.org/stable/10.1086/679562.

Fritz, Allhoff, Adam Henschke, and Bradley Jay Strawser. 2016. *Binary Bullets: The Ethics of Cyberwarfare.* New York: Oxford University Press.

Glanville, Luke. 2014. *Sovereignty and the Responsibility to Protect: A New History.* University of Chicago Press.

Hurka, Thomas. 2005. "Proportionality in War." *Philosophy and Public Affairs* 33 (1): 34-66.

I24 News. 2025. *PM Netanyahu to i24NEWS: We would have struck Iran even without the US.* https://www.i24news.tv/en/news/israel/defense/artc-pm-netanyahu-we-would-have-struck-iran-even-without-the-us.

IAEA. 2025. *Statement on the Situation in Iran.* https://www.iaea.org/newscenter/statements/statement-on-the-situation-in-iran-13-june-2025.

International Committee of the Red Cross (ICRC). 1977. *Protocol I to the Geneva Conventions.* https://ihl-databases.icrc.org/en/ihl-treaties/api-1977.

___. 1996. *Protocol II to the 1980 CCW Convention.* https://ihl-databases.icrc.org/en/ihl-treaties/ccw-amended-protocol-ii-1996?activeTab=.

___. 1868. *The Declaration of Saint Petersburg.* https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868.

Issacharoff, Samuel, and Richard H. Pildes. 2013. "Targeted warfare: Individuation enemy responsibility." *New York University Law Review* Volume 88.

Kotzur, Markus. 2009. *Max Planck Encyclopedias of International Law.* https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1412?prd=MPIL.

Krishnan, A. 2009. *Killer robots: legality and ethicality of autonomous weapons.* Farnham: Ashgate.

Kymlicka, Will. 2002. *Contemporary Political Philosophy.* 2nd ed. Oxford: Oxford University Press.

Lango, John W. 2014. "The Ethics of Armed Conflict. A Cosmopolitan Just War Theory. Chapter 8. Proportionality and Authority." 178-199. Edinburgh University Press. https://www.jstor.org/stable/10.3366/j.ctt9qdrf3.11.

Lister, Tim, and Salma Abdelaziz. 2014. *Israeli military's 'knock on roof' warnings criticized by rights groups.* July 15. https://edition.cnn.com/2014/07/15/world/meast/mideast-israel-strike-warnings/index.html?utm_source=chatgpt.com.

Lucas, George. 2017. *Ethics and Cyber Warfare: The Quest for Responsible Security in the Age of Digital Warfare.* New York: Oxford University Press.

Magramo, K., A. Renton, C. Edwards, P. Wilkinson, A. Sangal, D. Andone, and M. Chowdhury. 2023. "Israel seemingly stops "knock on the roof" military tactic. Here's what it means and why it matters." *CNN.* https://edition.cnn.com/middleeast/live-news/israel-hamas-war-gaza-10-11-23#h_b213ec9e2882bc819f20cb6a96bcec92.

Matthias, A. 2004. "The responsibility gap." *Ethics and Information Technology* 6 (3): 175–183.

May, Larry. 2012. *After War Ends: A Philosophical Perspective.* esp. 2–3. Cambridge: Cambridge University Press.

Miller, David. 2008. "Political Philosophy for Earthlings." In *Political Theory: Methods and Approaches*, edited by David Leopold și Marc Stears, 29-48. Oxford: Oxford University Press.

Moss, Stephen. 2003. *The paper war.* 6 March. https://www.theguardian.com/politics/2003/mar/06/iraq.foreignpolicy?utm_source=chatgpt.com.

Nafziger, James A. R. 1976. "Law and Responsibility in Warfare: The Vietnam Experience." *The American Journal of International Law* 70 (4): 866-868.

Nalin, LTC Alessandro, and Paolo Tripodi. 2023. "Future Warfare and Responsibility Management in the AI-based Military Decision-making Process." *Journal of Advanced Military Studies* 14 (1): 83-97. doi:10.21140/mcuj.20231401003.

Newsonair. 2025. *IAEA confirms no radiation spike after U.S. strikes on Iranian nuclear sites.* https://www.newsonair.gov.in/iaea-confirms-no-radiation-spike-after-u-s-strikes-on-iranian-nuclear-sites.

Reinold, Theresa. 2011. "State weakness, Irregular warfare, and the Right to Self-Defense post- 9/11." *American Journal of International Law* 105 (2): 244-286. https://www.jstor.org/stable/10.5305/amerjintelaw.105.2.0244.

Roberts, Adam. 2008. "Chapter 12: The Principle of Equal Application of the Laws of War." În *Just and Unjust Warriors*, editor David Rodin și Henry Shue, 226-254. Oxford University Press.

Robillard, Michael. 2011. *Persons, War, and Structures: A Case for Structural Responsibility as Applied to Warfare.* University of Victoria.

Rogers, A.P.V. 2000. "Zero-casualty warfare." *International Review of the Red Cross* 82 (837): 165-181. https://doi.org/10.1017/S1560775500075453.

Ruys, Tom. 2010. *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice.* Cambridge: Cambridge University Press.

Sassoli, M., and A. Bouvier. 1999. *How Does Law Protect in War?* Geneva: International Committee of the Red Cross.

Sauer, Frank, and Niklas Schörnig. 2012. „Killer drones: The 'silver bullet' of democratic warfare?" *Security Dialogue* 43 (4): 363 –380. doi:10.1177/0967010612450207.

Seddon, Sean, and Gabriela Pomeroy. 2025. *What we know about Iran's attack on US base in Qatar.* https://www.bbc.com/news/articles/cdjxdgjpd48o.

Shea, Jamie. 1999. *NATO press briefing on 26 March 1999.* www.nato.int.

Shue, Henry. 2008. „Chapter 5: Do We Need a 'Morality of War'?" In *Just and Unjust Warriors*, editor David Rodin and Henry Shue, 87-111. Oxford University Press.

Simons, Greg, and Iulian Chifu. 2017. *The Changing Face of Warfare in the 21st Century.* London and New York: Routledge Publishing House.

Singer, P.W. 2010. *Wired for war: the robotics revolution and conflict in the 21st century.* New York: Penguin.

Singer, Peter W., and Allan Friedman. 2013. *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Sirjani, Farhad Shahabi. 2013. "Iran's Nuclear Fatwa." *Iranian Review of Foreign Affairs* 4 (2): 57-80. https://ciaotest.cc.columbia.edu/journals/irfa/v4i2/f_0029607_23960.pdf.

Sparrow, R. 2007. "Killer robots." *Journal of Applied Philosophy* 24 (1): 62-77. https://doi.org/10.1111/j.1468-5930.2007.00346.x.

Taylor, P.M. 2007. *PSYOPS in Iraqi Freedom by Prof Taylor.* University of Leeds, School of Media and Communication. https://universityofleeds.github.io/philtaylorpapers/vp0186cd.html.

The White House. ___. 2025a. *Iran's Nuclear Facilities Have Been Obliterated — and Suggestions Otherwise are Fake News.* https://www.whitehouse.gov/articles/2025/06/irans-nuclear-facilities-have-been-obliterated-and-suggestions-otherwise-are-fake-news.

___. 2025b. *Iran's Nuclear Facilities Have Been Obliterated — and Suggestions Otherwise are Fake News.* https://www.whitehouse.gov/articles/2025/06/irans-nuclear-facilities-have-been-obliterated-and-suggestions-otherwise-are-fake-news/.

___. 2025c. *Experts Agree: Iran's Nuclear Facilities Have Been Obliterated.* https://www.whitehouse.gov/articles/2025/06/experts-agree-irans-nuclear-facilities-have-been-obliterated/.

Trooboff, Peter D. 1975. *Law and Responsibility in Warfare: The Vietnam Experience.* Edited by Chapel Hill: The University of North Carolina Press, under the auspices of the American Society of International Law.

UN Peacemaker. 1996. "Agreement on a Ceasefire, the Cessation of Military Activities, and on Measures for a Settlement of the Armed Conflict on the Territory of the Chechen Republic." https://peacemaker.un.org/sites/default/files/document/files/2024/05/ru960527agreement20on20a20ceasefire.pdf.

United Nations. 1949. *Geneva Convention relative to the Protection of Civilian Perons in Time of War.* https://www.ohchr.org/en/instruments-mechanisms/instruments/geneva-convention-relative-protection-civilian-persons-time-war.

___. 1951. *Convention on the Prevention and Punishment of the Crime of Genocide.* https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.1_Convention%20on%20the%20Prevention%20and%20Punishment%20of%20the%20Crime%20of%20Genocide.pdf.

___. 1968. *Treaty on the Non-Proliferation of Nuclear Weapons (NPT).* https://legal.un.org/avl/ha/tnpt/tnpt.html.

___. 2001. *United Nations Treaties Against Terrorist.* https://www.ohchr.org/en/press-releases/2009/10/united-nations-treaties-against-international-terrorism.

___. 2005. *Resolution adopted by the General Assembly on 16 September 2005.* https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_RES_60_1.pdf.

___. 2007. "Letter dated 31 August 2007 from the Secretary-General addressed to the President of the Security Council." S/2007/721. https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/Gen%20S2007%20721.pdf.

___. 2011a. *Resolution 1970 (2011).* https://docs.un.org/en/S/RES/1970%20(2011).

___. 2011b. *Resolution 1973 (2011).* https://docs.un.org/en/S/RES/1973%20(2011).

US Department of State. 2009. *Country Reports on Terrorism 2008.* https://2009-2017.state.gov/j/ct/rls/crt/2008/122412.htm.

Walzer, M. 1977. *Just and unjust wars: a moral argument with historical illustrations.* New York: Basic.

Williams, Andrew. 1998. "Incentive, Inequality and Publicity." *Philosophy & Public Affairs* 27: 225–247.

Withnall, A. 2014. *Israel-Gaza conflict: Israeli 'knock on roof' missile warning revealed in remarkable video.* https://www.independent.co.uk/news/world/middle-east/israelgaza-conflict-israeli-knock-on-roof-missile-warning-technique-revealed-in-stunning-video-9603179.html.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Visual Lessons: How AI Is Revolutionizing English Learning

Assoc.prof. Ana-Maria CHISEGA-NEGRILĂ*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: anachisega@gmail.com

Abstract

The use of AI media has become extremely popular in recent years due to its versatility and ability to create images and videos from written prompts. This versatility has opened the door for AI in teaching and learning, boosting its use as a tool to enhance students' motivation. The use of AI-generated media for teaching English draws on its playful nature, transforming learning into a form of interactive play. With AI, teachers can now produce compelling visuals, engaging stories, and interactive resources that help learners improve their language skills. Rather than relying solely on textbooks and traditional exercises, which may feel outdated to students, AI enables learners to acquire new vocabulary and develop listening, speaking, and writing skills in a dynamic way.

This paper explores the potential of materials generated by AI in teaching English, with a focus on their applicability in current classroom activities. It begins with a brief history of AI-generated images and an overview of current platforms for creating AI images and videos that teachers can incorporate into their lessons. The examples discussed include the use of images and videos for introducing vocabulary and practicing pronunciation, as well as writing exercises that use AI-generated media to foster students' creativity and confidence. The paper is based on teaching experience and practical observations, emphasizing the playful nature of AI and its ability to increase learners' engagement.

Keywords:

Artificial Intelligence; Education 4.0; Language Learning;
AI-generated images; AI-generated videos.

Article info

Received: 23 July 2025; Revised: 26 August 2025; Accepted: 11 September 2025; Available online: 6 October 2025

Citation: Chisega-Negrilă, A.M. 2025. "Visual Lessons: How AI Is Revolutionizing English Learning"
Bulletin of "Carol I" National Defence University, 14(3): 307-317. https://doi.org/10.53477/2284-9378-25-50

The development of artificial intelligence has deeper roots than is often believed, with early ideas of automation inspired as far back as mechanisms like the Jacquard loom (1804) and the mathematical projects of Charles Babbage and Ada Lovelace in the 19th century (Grzybowski, Pawlikowska–Łagód and Lambert 2024). However, modern AI saw a decisive advancement with the introduction of generative adversarial networks (GANs), proposed by Goodfellow and his collaborators (Goodfellow, et al. 2014), which paved the way for generating realistic images. Subsequent models, such as those proposed by Denton (Denton, et al. 2015), Li and Wand (Li and Wand 2016), and StyleGAN developed by Karras and colleagues (Karras, Laine and Aila 2018), further refined the quality and visual realism of AI-generated images.

A turning point came with the launch of DALL·E by OpenAI in 2021, which introduced image generation based on textual instructions (OpenAi 2025). This approach expanded AI accessibility beyond specialist circles, allowing the general public, including teachers and students, to use creative tools such as DALL·E 2 and 3, Midjourney, Stable Diffusion, or Adobe Firefly.

These developments did not remain solely in the technological sphere but quickly found applications in education. In particular, foreign language teaching benefits from visual and interactive resources generated by AI, which can support the learning process through playful, motivational, and personalized elements. This paper examines how these tools can be used in teaching English, with a focus on the advantages observed in classroom practice.

1. The Evolution of Video/Image Generation with Artificial Intelligence and Current Models

Before discussing the practical applications of AI in teaching, it is useful to contextualize its evolution through a brief history of AI-generated video and image creation, along with an overview of some currently used models.

AI's ability to generate images was first to develop, and it moved forward quite rapidly, so, for some time, AI-generated video seemed to lag behind, being able to generate only simple animations or static images with motion. This situation did not last long, and soon, with the progress in algorithms and with more powerful computing resources, things began to improve. One of the organizations involved in building tools for AI video generation was DeepMind, which came in 2017 with First-Person Video Generation, which allowed users to create extremely realistic videos using only simple input. However, as highlighted by Tulyakov (Tulyakov, et al. 2017), problems still remained when it came to obtaining coherent video sequences or complex scenarios with smooth transitions. Despite these limitations, the progress was significant and laid the foundation for further developments in AI video generation, in terms of quality, realism, and length.

2019 marked the turning point for video generation with the release of RunwayML, a platform that offered AI-friendly tools for users (Nanda 2019). RunwayML introduced easy-to-use interfaces for AI models that allowed creators to generate and edit video content with the help of Gen-2 and later Gen-3 models. DeepMind's Veo offered creators to possibility to generate videos from text, modify existing footage, and even generate synthetic media. These models used powerful machine learning techniques such as recurrent neural networks (RNNs) and temporal GANs to generate coherent motion and enhance video realism (Runwayml 2025).

Another important player is OpenAI's SORA, which has rapidly become one of users' favorite models for generating quality videos based on written prompts. The way SORA works is through a combination of language models and video synthesis techniques to generate videos that encapsulate the textual input. Sora creates short, high-quality videos not only from text, but also from images, or other existing footage, and is built on diffusion and transformer technologies with the purpose of obtaining visual consistency by following the prompts as closely as possible (OpenAi 2025).

By 2025, Hailuo by Minimax and other emerging platforms were pushing the boundaries even further, shaping creators' golden dream: to generate complex videos/images with simple input. These tools, coupled with intuitive user interfaces, became especially popular among non-experts, who had difficulties using previous models due to their complexity and opacity to neophytes.

Today, AI tools for image and video generation are used widely across industries, perhaps too much for the humanities' good, some might say, as DALL·E 3, Midjourney, and Stable Diffusion have become important tools in the design, advertising, or entertainment sectors. Their popularity is rooted in the fact that content creators can now produce visuals that were once time-consuming or expensive to create manually. Platforms like RunwayML, SORA, and DeepMind's Veo 2 are now popular among filmmakers and animators, and Midjourney (Midjourney 2025) has gained traction for its ability to produce a large array of images that often seem to be hand-crafted.

Technology continues to advance, and the natural outcome is that these AI models will intertwine more and more with professional workflows, due to the quality of results and reduced production time. For artists and designers, this may come as good news, as these tools will boost their creativity and offer the possibility to experiment more with ideas and different styles, a process that otherwise would have been more time-consuming. In the marketing, advertising, and film industry, AI also proves to be a winner due to its high-quality results and better time management when it comes to pre-visualization, and even to the production of fully cinematic sequences.

However, despite these innovations, some challenges still remain, especially ethical concerns related to copyright and ethics, but also to fairness, transparency, and

safety (Chaudhry, Cukurova and Luckin 2022). Deepfake technologies, for instance, have raised concerns about identity representation and consent, emphasizing the need for robust ethical frameworks to prevent misuse and misrepresentation (Leben 2024). Now, the very role of human creativity is put into question, and, especially, whether AI will replace humans completely or will only function as an alternative to traditional artistic methods.

Many legal systems have to deal with the implications of AI-generated works. A notable case in the U.S. District Court for the District of Columbia highlighted that while copyright laws are adaptable, human creativity remains central to copyrightability, underscoring the complexities of attributing authorship to AI-generated content (Lim 2023).

Despite these concerns, AI is currently seen as a tool that can improve human creativity rather than replace it. Studies from institutions like the University of Oxford (Ploin, et al. 2019) suggest that AI can serve as a collaborative partner in the creative process, enhancing artistic expression without replacing the unique contributions of human artists. An optimistic conclusion is that, even if AI models become more refined, they will more likely enhance, rather than replace, human creativity.

2. Using AI Video and Images for Learning

Even if AI has not replaced artists so far, it has transformed art into a mass phenomenon. As AI tools are more accessible, more people than ever before have begun to create visual art, music, and stories without having access to advanced technical skills or expensive resources. The barrier between professionals and dilettantes is fading away, and the only real limit is human imagination. This democratization of creativity means that art is no longer confined to trained employees and that anyone with an idea can experiment and share their work with the world. As a result, we are on the verge of a new era in which creativity is not a privilege but a widespread capacity empowered by technology.

Following this trend, educators, too, have begun to adopt AI-generated texts and images in the classroom educațional (Wang, et al. 2025). The main advantage of these tools is that they can bring abstract concepts to life, thus supporting better personalized learning experiences and helping students to express ideas in new ways. By integrating AI into teaching, educators can now find ways to engage learners and introduce new dimensions to learning, such as creativity and entertainment, as AI tools used to generate images and videos have become popular not only on social media but also for learning. For example, AI-generated images and videos can provide visual demonstrations, illustrate vocabulary, historical events, but also more abstract scientific concepts, making them easier to understand and remember.

In (Kim, Lee and Cho 2022), teachers identified a three-stage progression for how students are expected to collaborate with AI: first, learning about AI, where students build up knowledge of how AI works, second, learning from AI, in which students use AI tools as an educational resource, and third, learning with AI, where students and AI cooperate to draft creative solutions, this representing a shift from understanding AI to engaging with it in a collaborative way.

Moreover, AI models that generate images and videos encourage creativity and critical thinking as learners can use them to create their own content, such as visual essays or video projects. This approach reinforces language acquisition because students interact with the AI via prompts, having to modify their text if the visual content obtained is not the one desired, and thus refining their understanding of grammar and vocabulary. This ability will make learning more engaging, as students will also produce their own images and videos and will have the satisfaction of obtaining an instant and tangible outcome from their endeavor.

2.1. Visual Context for Vocabulary

AI-generated images can be used to learn English vocabulary or review the previously acquired words when students associate them with their visual representation. Their memory retention improves if, for instance, when learning the word "elephant," an AI-generated image of an elephant will help learners connect the word with a tangible visual, making the word easier to remember. However, AI-generated images are also valuable when it comes to illustrating complex or abstract terms that are more difficult to understand through words alone. Words such as "freedom," "justice," or "ecosystem" may not have clear, straightforward images associated with them, but an AI tool can create visuals that embody the essence of these concepts, thus adding a layer of understanding that textual explanations might lack. AI-generated images will help learners remember certain words and also gain a better understanding of their meanings and usage in different contexts. Therefore, this method can be used especially with language learners who encounter problems with traditional textbook definitions, offering them a more attractive way to acquire new vocabulary.

2.2. Listening and Pronunciation Practice

AI-generated films, especially those with voiceovers, are a powerful way to practice listening and pronunciation. These films expose learners to natural language, helping them improve their comprehension and pronunciation as hearing sentences spoken by AI models familiarizes them with the intonation and flow of native speakers placed in real-world contexts.

Among the examples of AI platforms are RunwayML, Synthesia, and Elevenlabs, which can assist teachers in creating AI-generated films with voiceovers. Synthesia, for example, allows the creation of videos with AI avatars who speak text in natural-sounding voices, making it an ideal tool for practicing listening, as users can adjust

the speed of speech or replay sections to focus on certain fragments. For instance, learners can repeat phrases or pause and replay sections to focus on specific sounds and syllables. Elevenlabs, DeepL, and Google's Text-to-Speech are other tools that can generate accurate voiceovers for language learners, helping them practice pronunciation by listening to clear, natural speech.
With regular practice, exposure to generated videos with voiceover can significantly improve not only comprehension but also the ability to speak, as students will gain confidence regarding their pronunciation and fluency.

2.3. Creative Writing Prompts

AI-generated images are also a good resource for stimulating creativity and improving writing skills. These images came in different styles and can be created with vivid details so that they will inspire learners to create stories or essays based on what they see. For example, an AI-generated image can serve as the foundation for a narrative in which learners will build characters, settings, and plots, but a visual prompt may also serve other purposes, such as overcoming writer's block or giving learners a starting point, making it easier for them to focus on developing their ideas and refining their writing. Research shows that AI-generated visuals can enhance story creativity and originality, making them an effective tool for educational use (Ali and Parikh 2021).

DALL·E 3, Midjourney, and Artbreeder are only some examples of platforms for generating images that can serve as creative prompts for writing or speaking. These platforms function with input text descriptions, resulting in images that match users' ideas and offer a wide range of visual options that can be later tailored to create writing exercises. Educational blogs and platforms have highlighted the benefits of combining writing with AI visuals to support student engagement and idea development (Microsoft Designer 2024). Once learners have an image, they can use it as inspiration to write stories or create character descriptions, but AI can also create a succession of images that differ more or less, so learners can improve not only their writing but also their speaking by comparing or contrasting them. This approach not only strengthens writing skills but also improves learners' critical thinking, as they analyze the images and then translate them into written/spoken form.

2.4. Interactive Learning

Some AI tools prove to be an extremely engaging, and sometimes addictive, form of interactive learning because they allow learners to modify text prompts and observe how the generated images or videos change accordingly. The result is that students experiment with language, thus practicing their vocabulary, grammar, and syntax as they get immediate visual feedback and are motivated to continue their attempts, as learning and creativity go hand in hand. For instance, a learner could modify the description of a scene by changing adjectives or sentence structures, and immediately see the impact on the AI-generated images, this dynamic interaction helping learners understand the relationships between words and their visual counterparts.

DALL·E 3, RunwayML, and Stable Diffusion allow users to adjust their prompts while getting real-time feedback. When modifying prompts, learners experiment with language and see how slight modifications, such as changing tense or using synonyms, affect the final output. The same situation applies to AI-generated videos on platforms like Synthesia or Runway, which allow learners to tweak scenes or dialogues, thus improving their understanding of how context, register, and syntax work together in storytelling. Ultimately, this interactive learning process makes language practice more engaging and effective, resulting in an increase in students' motivation.

2.5. Engagement and Motivation

As seen above, the AI-generated content can have a positive impact on learner engagement by making language practice more fun and interactive. When teachers include interactive elements in lessons, learners are more likely to stay motivated and interested in their studies due to their involvement in the teaching-learning process and freedom to personalize content, generate images or videos that match their learning interests. Learners might generate visual representations of their own stories, characters, or scenarios, which adds an element of creativity and excitement to the learning process as learners get actively involved in their learning, rather than passively absorbing information.

DALL·E 3 and RunwayML, but also other platforms, encourage this type of creativity, which, besides the creative dimensions, adds another layer to learning. On the one hand, students feel a sense of accomplishment and ownership over the learning experience, which boosts motivation; on the other, AI-generated content can be tailored to individual preferences, making lessons more enjoyable. Whether through interactive storytelling, visual challenges, or video creation, AI tools introduce an element of play and exploration into learning English, making it feel less like a traditional classroom exercise and more like an engaging, modern, and enjoyable activity.

3. Using AI-Generated Images for Learning New Vocabulary

Let's consider how AI-generated images can be effectively used in a lesson focused on teaching English vocabulary and creative writing to students. The goal of this lesson is to help them expand their vocabulary, improve descriptive writing skills, and improve their understanding of grammar and sentence structure with the help of AI-generated images.

3.1. Introducing New Vocabulary

The teacher introduces the new vocabulary related to "military operations" or "security," and chooses words like *soldier, base, mission, patrol*, and *convoy*.

Then, the teacher uses a platform like DALL·E 3 or Midjourney and generates images in order to reinforce these words.

For example:

An image of a soldier in full gear standing at attention.
A military base with vehicles lined up.
A convoy moving across rough terrain.

3.2. Exploring Context through Visuals

The teacher shows students the images and asks them to write descriptions while encouraging them to use the given vocabulary. For example:

The soldier is wearing a helmet and body armor. He is ready for the mission.
The base has tall watchtowers and security fences.

The teacher can guide the students to create more descriptive sentences, telling them to use more adjectives and adverbs and use the details in the pictures.

3.3. Grammar and Sentence Structure Practice

Once the students have finished writing their descriptions, the teacher will explain grammar or sentence structures. For example:

Simple sentences: *The soldier is prepared.*
Complex sentences: *The convoy moves through the desert while the patrol watches the road.*
Use of adjectives: *The base is heavily fortified and carefully guarded.*

The teacher can ask students to imagine a plot that connects more images, like a picture of a soldier boarding a helicopter, another one of a mission in progress, the same soldier returning to camp, and encourage them to ask questions to find out more information regarding the situation. The students will ask questions using different tenses:

Who is he?
Where is he?
What is he doing?
When did he start the mission?

3.4. Creative Writing Prompts

After everything has been explained and the students have asked and answered questions, the teacher gives them a prompt based on one of the images that were generated with AI. For example:

Write a short story that begins with a soldier entering a base. Describe what he/she sees, hears, and feels. Use at least five words from today's lesson.

or

Imagine you are part of a convoy on patrol and write a diary entry about the mission, describing both the environment and your emotions.

The function of the image is to boost students' imagination and make them practice the newly acquired knowledge in a pleasant way.

3.5. Peer Review and Feedback

After completing their writing, students are asked to choose a classmate and give the description for peer review. The other student can use the AI-generated images to provide feedback and to discuss how well the descriptions and the visual representation match, helping both students reflect on their use of vocabulary and sentence structures. For example, they might point out the things that can be improved:

> *You did a great job describing the soldier, but I think you could add more detail about his equipment.*
> *The base scene was very good, but you could include more sensory details, for instance, what sounds the convoy makes as it moves.*

3.6. Final Review

To conclude the lesson, the teacher can use the AI-generated images once again as an exercise in which the students could be asked to revise their original descriptions or stories based on feedback. This will help reinforce both vocabulary and writing, while students will see how their writing can be improved if details are added.

Benefits of Using AI Images in This Lesson:
Enhanced Vocabulary: Students connect words with images, a fact that will improve retention.

- Contextual Understanding: Students see the vocabulary in action, making it easier to understand how to use the words in different contexts.
- Creative Exploration: AI-generated images boost creativity and encourage students to write better stories.
- Grammar Practice: The images give students a clear context to apply and reinforce grammar rules such as sentence structure, tenses, adjectives, etc.

In the end, educators will provide more interesting lessons if they include AI-generated images into vocabulary and writing exercises, helping students become more aware of their learning and improving their understanding of language in a both creative and enjoyable way.

Conclusion

AI-generated images and videos are not only popular but they are also a powerful tool for enhancing education, especially when it comes to language learning. When educators use AI resources in their lessons, they provide students with a more engaging experience that, in the end, will foster creativity and critical thinking. AI-generated content can be used in many situations, but the present article concentrated only on some aspects regarding the use of AI images to put the new vocabulary in a visual context, support grammar practice, and make students write better descriptions.

AI tools are flexible, and they allow students to modify prompts and obtain instant changes, which results in promoting active learning so that learners will remain motivated. The ability to create personalized content encourages students to explore language in a new way, leading to improved writing, listening, and speaking skills. Regardless of their use: for vocabulary building, creative writing, or interactive grammar exercises, AI images and videos make learning more attractive, and as AI technology continues to evolve, its potential for education is almost unlimited.

References

Ali, Safinah, and Devi Parikh. 2021. „Telling Creative Stories Using Generative Visual Aids." Edited by ArXiv abs/2110.14810. *Proceedings of the AAAI Conference on Artificial Intelligence.* doi:10.48550/arXiv.2110.14810.

Chaudhry, MA, M Cukurova, and R Luckin. 2022. "A Transparency Index Framework for AI in Education." *Artificial Intelligence in education: posters and late breaking results, workshops and tutorials, industry and innovation tracks, practitioners and doctoral consortium, pt II*, 195-198. doi:10.1007/978-3-031-11647-6_33.

Chen, Lijia, Pingping Chen, and Zhijian Lin. 2020. "Artificial Intelligence in Education: A Review." *IEEE Access,* 75264-75278. Accessed 06 4, 2024. doi: 10.1109/ACCESS.2020.2988510.

Denton, Emily, Soumith Chintala, Arthur Szlam, and Rob Fergus. 2015. "Deep Generative Image Models using a Laplacian Pyramid of Adversarial Networks." *CoRR* abs/1506.05751: 1-10. http://arxiv.org/abs/1506.05751.

Goodfellow, Ian J., Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. 2014. "Generative Adversarial Nets." *Advances in Neural Information cessing Systems* 2672-2680. doi:10.48550/arXiv.1406.2661.

Grzybowski, Andrzej, Katarzyna Pawlikowska–Łagód, and W. Clark Lambert. 2024. "A History of Artificial Intelligence." *Clinics in Dermatology* 42 (3): 221-229. https://doi.org/10.1016/j.clindermatol.2023.12.016.

Karras, Tero, Samuli Laine, and Timo Aila. 2018. "A Style-Based Generator Architecture for Generative Adversarial Networks." *CoRR*. http://arxiv.org/abs/1812.04948.

Kim, Jinhee, Hyunkyung Lee, and Young Hoan Cho. 2022. "Learning design to support student-AI collaboration: perspectives of leading teachers for AI in education." *Education and Information Technologies*, 6069–6104. https://doi.org/10.1007/s10639-021-10831-6.

Leben, Derek. 2024. *Deepfakes and the Ethics of Generative AI.* https://tepperspectives.cmu.edu/all-articles/deepfakes-and-the-ethics-of-generative-ai/#:~:text=Generative%20AI%20technologies%2C%20like%20those%20used%20to%20clone,representation%2C%20consent%2C%20and%20the%20growing%20threat%20of%20deepfakes.

Li, Chuan, and Michael Wand. 2016. "Combining Markov Random Fields and Convolutional Neural Networks for Image Synthesis." *CoRR* abs/1601.04589: 1-10. http://arxiv.org/abs/1601.04589.

Lim, Daryl. 2023. "Generative AI and copyright: principles, priorities and practicalities." *Journal of Intellectual Property Law & Practice*, 12: 841-842. https://doi.org/10.1093/jiplp/jpad081.

Microsoft Designer. 2024. *AI-Powered creativity with Microsoft Designer.* https://microsoft.design/articles/ai-powered-creativity-with-microsoft-designer/.

Midjourney. 2025. *Documentation.* https://docs.midjourney.com/hc/en-us/categories/32013335627533.

Nanda, Vipul. 2019. "Runway ML – Harnessing AI to augment creativity." *Techweek.* 23 09. https://techweek.com/runway-ml-ai-creators-design/.

NVIDIA. 2025. *StyleGAN3 pretrained models.* https://catalog.ngc.nvidia.com/orgs/nvidia/teams/research/models/stylegan3.

OpenAi. 2025. *Sora System Card.* https://openai.com/index/sora-system-card/.

Ploin, Anne, Rebecca Eynon, Isis Hjorth, and Michael A. Osborne. 2019. "Art for our sake: artists cannot be replaced by machines." Creative Algorithmic Intelligence Research Project, Oxford Internet Institute, Oxford. https://eng.ox.ac.uk/news/new-report-into-the-intersection-of-ai-and-the-arts/.

Runwayml. 2025. *Building general-purpose multimodal simulators of the world.* https://runwayml.com/research.

Tulyakov, Sergey, Ming-Yu Liu, Xiaodong Yang, and Jan Kautz. 2017. "MoCoGAN: Decomposing Motion and Content for Video Generation." *CoRR* 1-13. http://arxiv.org/abs/1707.04993.

Wang, Yi, Ziting Wei, Tommy Tanu Wijaya, Yiming Cao, and Yimin Ning. 2025. "Awareness, acceptance, and adoption of Gen-AI by K-12 mathematics teachers: an empirical study integrating TAM and TPB." *BMC Psychology*, 1-14. https://doi.org/10.1186/s40359-025-02781-2.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats

Sorina-Denisa POTCOVARU (DRAGNE), PhD Candidate*
Professor Marinel-Adi MUSTAȚĂ, PhD**

*Interdisciplinary Doctoral School, "Carol I" National Defence University, Bucharest, Romania
e-mail: sorina.potcovaru@yahoo.com
**Faculty of Security and Defence, "Carol I" National Defence University, Bucharest, Romania
e-mail: mustata.adi@unap.ro

Abstract

The complexity of the interaction between critical infrastructures and hybrid threats emerges in the specialized literature through a diversity of perspectives and approaches. This study investigates how the two concepts intersect, highlighting hybrid manifestations that combine cyberattacks, disinformation campaigns, kinetic operations, economic coercion, and the exploitation of legal grey zones in international law. At the same time, critical infrastructures are analyzed both as strategic targets and as instruments for the propagation of hybrid threats, being weaponized through the exploitation of their sectoral and inter-sectoral vulnerabilities, and thus generating cascading effects. Examples from the literature highlight not only the cyber and economic dimensions of such hybrid actions but also the difficulties of attribution and the multidimensional nature of the typology of the actors involved. The conclusions of the article emphasize the necessity of understanding hybrid threats and critical infrastructures as interconnected realities, whose protection and resilience require a systemic and coordinated approach, capable of responding to the complex challenges of contemporary security.

Keywords:
Hybrid Threats; Critical Infrastructures; Interdependencies; Cyberattacks; Disinformation; Economic Coercion; Weaponizing; Resilience.

Article info
Received: 1 August 2025; Revised: 2 September 2025; Accepted: 15 September 2025; Available online: 6 October 2025

Citation: Potcovaru (Dragne), S.D., and M.A. Mustață. 2025. "From Targets to Tools: the Complex Relationship between Critical Infrastructures and Hybrid Threats." *Bulletin of "Carol I" National Defence University*, 14(3): 318-327. https://doi.org/10.53477/2284-9378-25-51

The transformations of the international security environment have brought hybrid threats to the forefront, defined by the combination of conventional and unconventional, military and non-military means, employed to exploit the vulnerabilities of states and international organizations with the purpose of destabilizing democratic societies to the advantage of hostile state and non-state actors. In this context, critical infrastructures occupy a central position, both through their essential role in ensuring the functioning of modern societies and through their high degree of interdependence and exposure to complex attacks.

The literature emphasizes that critical infrastructures are simultaneously strategic targets and channels for the propagation of hybrid threat vectors within democratic societies. Cyberattacks, disinformation campaigns, kinetic operations, economic coercion, as well as actions conducted in "grey zones," represent the main modalities through which state and non-state actors exploit these vulnerabilities. At the same time, the concept of critical infrastructure is approached in the literature from multiple perspectives, general, sectoral, and inter-sectoral, reflecting the diversity of analytical frameworks and understandings of the phenomenon.

This study aims to analyze the manifestation of hybrid threats against critical infrastructures, drawing on three major directions identified in the literature: (1) the conceptualization of critical infrastructures, from general to sectoral approaches; (2) the conceptualization and operationalization of hybrid threats; and (3) the relationship between critical infrastructures and hybrid threats. This structure allows for the highlighting of the complexity of the phenomenon and the outline of a comprehensive picture of the current challenges to the resilience of critical infrastructures in the face of hybrid threats.

The present article is based on an analysis of the literature addressing the manifestation of hybrid threats against critical infrastructures. The literature includes scientific articles indexed in the Web of Science database (n=8) and research reports (n=10) developed under the auspices of the European Union, the North Atlantic Treaty Organization, and the European Centre of Excellence for Countering Hybrid Threats.

Critical Infrastructures, from General to Sectoral

The analysis of the specialized literature reveals that critical infrastructure is conceptualized differently depending on the degree of specificity adopted by researchers. Thus, three main directions can be distinguished: a general approach, which addresses critical infrastructure as a whole; an inter-sectoral approach, focused on the interdependencies between sectors; and a sectoral approach, oriented toward the vulnerabilities of a particular domain.
Studies adopting a general approach start from the premise that critical infrastructures, in their entirety, constitute strategic objectives for actors employing

instruments specific to hybrid threats. In this direction, Boyte (2017) highlights how cyberattacks can simultaneously affect government services, financial networks, and telecommunications systems, thereby generating systemic instability. In the same line, Mazaraki and Goncharova (2022) emphasize that digital interconnectivity facilitates the conduct of hybrid attacks in the legal "grey zone." Jukka (2019) also stresses the dependence of critical infrastructures on digital networks, which amplifies their exposure to hybrid threats. A complementary perspective is offered by Wigell, Mikkola, and Juntunen (2021), who argue for the necessity of a whole-of-society strategy to protect infrastructures in the context of cumulative effects produced by hybrid attacks targeting multiple sectors simultaneously. Conceptually, Giannopoulos, Smith, and Theocharidou (2021) integrate infrastructure into the general model of hybrid threats, treating it as a key domain of action.

Literature further underscores the interdependencies among infrastructures, identifying them as significant sources of vulnerability when confronted with hybrid threats. Aho, Midoes, and Šnore (2020) show how financial infrastructure becomes exposed due to its connections with the energy and telecommunications sectors. Similarly, Carlsson and Gustavsson (2017) analyze the dependence of the energy infrastructure on the telecommunications sector, identifying it as a vulnerability exploitable by hostile actors.

Fiott and Parkes (2019) underscore the central role of digital infrastructure, indispensable for the functioning of both civilian and military infrastructures, while also serving as a potential entry point for inter-sectoral attacks. Tessari and Muti (2021) focus on the interdependence between energy and telecommunications infrastructures, arguing that destabilization in these areas can simultaneously affect both national economies and defense capabilities. Nave et al. (2022) discuss inter-sectoral vulnerabilities between energy and transport infrastructures, particularly in the context of NATO cooperation in the Baltic Sea region. Similarly, Bueger and Liebetrau (2021) highlight the importance of submarine communication cables, on which critical domains such as telecommunications, finance, and defense depend.

Another direction explored in the literature concerns the focus on specific types of infrastructure. The Hybrid CoE report (2019) examines nuclear energy infrastructure as a strategic target for hybrid actors, given its dual-use applications in both civilian and military domains. Evans (2020) reaches a similar conclusion regarding energy networks, stressing the significant impact that a hybrid attack could have on both civilian and defense sectors.

Concerning communications infrastructure, Jokinen, Normark, and Fredholm (2022) analyze vulnerabilities that can be exploited by non-state actors. Maritime infrastructure is also a prominent target: Schaub, Murphy, and Hoffman (2017) demonstrate how ports and maritime communication lines can be attacked to disrupt global trade and military logistics. Jukka et al. (2019) emphasize the specific

vulnerabilities of submarine cables and maritime routes located in geopolitically sensitive regions. Along the same lines, Bueger et al. (2022) underline the dual-use character of submarine cables, which are essential for both civilian and military communications. Finally, Demertzis and Wolff (2020) examine the financial sector, pointing out weaknesses such as fragmented security and the excessive centralization of payment systems, banking structures, and insurance markets.

The three approaches, general, inter-sectoral, and sectoral, provide a complex picture of how critical infrastructure is analyzed in the context of hybrid threats. Although the approaches differ, a common theme emerges: interconnectivity. Whether analyzed at the macro, inter-sectoral, or sectoral level, the dependence between systems constitutes a fundamental source of vulnerability that hybrid actors exploit to generate effects with systemic impact.

The Operationalization of Hybrid Threats in Relation to Critical Infrastructures

The specialized literature addresses hybrid threats through a variety of concepts and modes of operation, with a common focus on exploiting the vulnerabilities of critical infrastructures. The analysis of studies reveals several recurring thematic directions: the centrality of the cyber dimension, the use of disinformation, the conduct of kinetic operations, economic coercion, the exploitation of grey zones, and issues of non-attribution. In parallel, the literature also examines the typology of actors involved, both state and non-state, and the relationships between them.

The cyber dimension consistently emerges as a central element of hybrid threats, particularly in connection with attacks on critical infrastructures. Boyte (2017) provides a comparative analysis of cyberattacks conducted by Russia-sponsored actors against financial, governmental, and telecommunications infrastructures in Estonia, the United States, and Ukraine. A distinctive feature of these operations is their execution in the digital "grey zone," where the difficulty of attribution complicates state responses (Mazaraki and Goncharova 2022). Carlsson and Gustavsson (2017) demonstrate the effectiveness of attacks on energy infrastructures, highlighting their dependency on digital networks. Other studies (Jukka 2019; Evans 2020) emphasize the vulnerabilities of dual-use infrastructures (civilian and military), especially in the energy and communications sectors.

The financial sector is likewise a privileged target: Aho, Midoes, and Šnore (2020) investigate how cyber espionage exploits vulnerabilities in payment systems, while Demertzis and Wolff (2020) note the intensification of cyberattacks against banks and stock exchanges, with the involvement of non-state actors.

Disinformation campaigns appear as amplifiers of the effects of hybrid threats on critical infrastructures. Wigell, Mikkola, and Juntunen (2021) argue that by

influencing public opinion, such campaigns can delay governmental responses. Tessari and Muti (2021) illustrate the synergy between disinformation and cyberattacks in the context of Europe's energy dependence on Russia. In the maritime sector, disinformation targets the security of ports and trade routes, generating economic insecurity (Schaub, Murphy and Hoffman 2017), while disinformation campaigns concerning submarine cables amplify the effects of both physical and cyberattacks (Bueger and Liebetrau 2021). Demertzis and Wolff (2020) further underline the combined impact of disinformation and social engineering in undermining public trust in financial institutions.

Hybrid threats also include physical components, complementing cyber operations. Examples include the sabotage of ports and submarine cables (Schaub, Murphy and Hoffman 2017; Bueger and Liebetrau 2021). Bueger et al. (2022) highlight the role of non-state actors, supported by Russia and China, in physical attacks against submarine cables, combined with cyber operations and the use of underwater drones. Moreover, nuclear energy infrastructure is an especially sensitive target, where hybrid attacks could generate major environmental and security consequences (Hybrid CoE 2019).

Economic coercion is analyzed as a specific instrument of state actors. Evans (2020) shows how China uses foreign direct investment to gain control over energy and telecommunications infrastructures. Fiott and Parkes (2019) discuss the vulnerability of the European Union's financial system to economic manipulation by external actors.

A key feature of hybrid threats is their conduct in "grey zones" and the challenge of attribution. Cyberattacks on infrastructures are often non-attributable (Mazaraki and Goncharova 2022), allowing hostile actors to exploit the time gained to carry out further actions (Hybrid CoE 2019). Jokinen, Normark, and Fredholm (2022) argue that non-state actors can function as state proxies, exploiting the lack of a well-defined legal framework. Similarly, Nave et al. (2022) underscore the persistence of legal ambiguity in the Baltic region, where both cyberattacks and acts of physical sabotage continue to resist clear legal categorization.
In most studies, Russia and China are identified as central state actors. Russia employs cyberattacks (Fiott and Parkes 2019; Boyte 2017), exploits infrastructural interdependencies (Jukka 2019), and applies energy pressures on Europe (Tessari and Muti 2021). China is analyzed in relation to cyberattacks against nuclear infrastructures (Hybrid CoE 2019) and its use of economic control through investment (Evans 2020).

Non-state actors include hacktivists and cyber mercenaries (Carlsson and Gustavsson 2017; Mazaraki and Goncharova 2022), as well as pirates or terrorist networks targeting maritime infrastructure (Bueger and Liebetrau 2021; Jukka, et al. 2019). In some cases, they collaborate with states, acting as proxies or auxiliaries (Evans 2020; Tessari and Muti 2021). Jokinen, Normark, and Fredholm (2022)

propose a detailed taxonomy, classifying non-state actors as proxies, auxiliaries, or surrogates, depending on their relationship with states.

The analysis of the literature confirms the multidimensional character of hybrid threats. Cyberattacks are recurrent and central, kinetic operations complement digital actions, disinformation amplifies effects, while the economic dimension and exploitation of grey zones reinforce the effectiveness of these tactics. Furthermore, the interaction between state and non-state actors makes it particularly difficult to identify perpetrators and to design effective response strategies.

The Relationship between Critical Infrastructures and Hybrid Threats

The specialized literature highlights a close connection between critical infrastructures and the manifestation of hybrid threats through an interconnected approach to these two concepts. The analysis of studies reveals three main thematic directions: critical infrastructures as targets, their use as weapons (weaponizing), and the exploitation of the economic and social vulnerabilities associated with them.

The vital nature of critical infrastructures makes them prime objectives for hybrid actors. Boyte (2017) shows that the cyberattacks carried out in Estonia, the United States, and Ukraine targeted infrastructures such as telecommunications, governmental services, and financial systems, with the aim of destabilizing state functions. In a similar analysis, Jukka (2019) underscores the systemic importance of infrastructures, noting that their interdependencies amplify the cascading effects generated when a single sector is attacked.

An additional source of vulnerability lies in the dual-use nature of critical infrastructures. Energy and communications networks, with both civilian and military applications, become strategic targets, affecting society and defense capabilities simultaneously (Evans 2020). Nuclear infrastructure is especially sensitive due to its potential for major impacts on both security and the environment (Hybrid CoE 2019).

Another thematic trend identified is the use of infrastructures not only as targets but also as instruments of hybrid threats. Evans (2020) defines weaponizing critical infrastructure as a long-term strategy aimed not merely at causing immediate disruptions but at undermining national security and defense capabilities. He provides examples of how Russia, China, Iran, and North Korea apply this strategy against energy, transport, telecommunications, and defense industry infrastructures, particularly targeting the United States and NATO member states.

Carlsson and Gustavsson (2017) further show that cyberattacks on energy infrastructures can force governments to allocate significant resources to restoring

services, diverting attention from a strategic response. The Coherent Resilience Baltic 2021 exercise illustrates how energy can be transformed into a tool for destabilizing regional cooperation and military alliances (Nave, et al. 2022). Similarly, the vulnerabilities of submarine cables are exploited to disrupt dependent infrastructures such as communications, financial systems, or even military operations.

The third thematic direction highlights how hybrid actors exploit the economic and social weaknesses associated with critical infrastructures. Russia, for instance, manipulates energy supply chains to create dependency and exert economic coercion in pursuit of geopolitical objectives (Tessari and Muti 2021). Similarly, financial infrastructure is exploited through tactics of coercion and manipulation: Aho, Midoes, and Šnore (2020) show how it can be destabilized by hybrid attacks, while Fiott and Parkes (2019) discuss external pressures designed to weaken the financial system of the European Union. Maritime infrastructure is also targeted to exploit the global dependence on trade, thereby generating economic and strategic instability at the international level.

Overall, the relationship between critical infrastructures and hybrid threats is characterized by a dual dimension: critical infrastructures are simultaneously targets and instruments. Interdependence, dual-use characteristics, and economic and social vulnerabilities increase the attractiveness of infrastructures for hybrid actors. This reality reinforces the argument that the protection of critical infrastructures must be addressed through a systemic and multidimensional approach.

Conclusions

The analysis of the specialized literature confirms that the relationship between critical infrastructures and hybrid threats is complex, multidimensional, and evolving. From a conceptual perspective, critical infrastructures are addressed in general terms as an interconnected system essential for the functioning of modern societies, as well as sectorally or inter-sectorally, depending on the specific vulnerabilities of each domain. This diversity reflects the recognition of the central role of infrastructures in the equation of contemporary security.

Hybrid threats manifest through a wide spectrum of actions, with the cyber dimension recurrent and dominant, complemented by disinformation, kinetic operations, and economic coercion. The exploitation of "grey zones" and the difficulty of attribution enhance the effectiveness of these actions, granting hostile actors the freedom to operate below the threshold of conventional armed conflict. Moreover, the interaction between state and non-state actors reinforces the challenging nature of countering such threats.

The relationship between critical infrastructures and hybrid threats can be approached through a dual dimension: critical infrastructures simultaneously

represent targets of hostile actions and instruments employed for the destabilization of states and alliances. Interdependence, dual-use characteristics, and economic and social vulnerabilities increase the attractiveness of infrastructures for hybrid actors, generating cascading effects at national, regional, and global levels.

Considering the analysis conducted, it becomes clear that critical infrastructures can no longer be regarded solely as vulnerable targets of hybrid threats but also as strategic instruments transformed and instrumentalized by hostile actors to generate destabilizing effects across multiple levels. This dual stance, of infrastructures as both objectives and weapons, illustrates the complexity of the phenomenon and highlights the interconnectedness of the two key concepts. Consequently, understanding the relationship between critical infrastructures and hybrid threats requires moving beyond a sectoral vision toward a systemic and integrated perspective, one that captures the dynamics through which vulnerability can be transformed into a lever of pressure and destabilization.
It follows that the protection of critical infrastructure in European democratic societies requires a systemic, multidimensional, and integrated approach that combines technological resilience, inter-institutional cooperation, and international coordination.

Furthermore, future research directions should capture the complexity of the phenomenon and promote the integration of sectoral approaches developed at NATO and the European Union levels. Future studies should investigate coordination mechanisms between these two organizations, explore inter-sectoral scenarios, and develop analytical tools capable of integrating the cyber, economic, informational, and legal dimensions of hybrid threats.

Only through such mechanisms can the destabilizing impact of hybrid threats be limited and the response capacities of states and democratic organizations be strengthened. The need for a systemic approach to the resilience of critical infrastructures derives from the structural interdependence of these systems and from the multidimensional character of hybrid threats.

References

Aho, Aleksi, Catarina Midões, and Arnis Šnore. 2020. *Hybrid Threats in the Financial System*. Hybrid CoE Working Paper 8. The European Centre of Excellence for Countering Hybrid Threats.

Boyte, Kenneth J. 2017. "A Comparative Analysis of the Cyberattacks Against Estonia, the United States and Ukraine." *International Journal of Cyber Warfare and Terrorism* 7(2): 1–15. https://doi.org/10.4018/ijcwt.2017040104.

Bueger, Christian, and Tobias Liebetrau. 2021. "Protecting Hidden Infrastructure: The Security Politics of the Global Submarine Data Cable Network." *Contemporary Security Policy* 42(4): 590–616. https://doi.org/10.1080/13523260.2021.1907129.

Bueger, Christian, Tobias Liebetrau, and Jonas Franken. 2022. *Security Threats to Undersea Communications Cables and Infrastructure – Consequences for the EU*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Carlsson, Anders, and Rune Gustavsson. 2017. "The Art of War in the Cyber World." In *2017 4th International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T)*, 453–456. https://doi.org/10.1109/INFOCOMMST.2017.8246345.

Demertzis, Maria, and Guntram Wolff. 2020. "Hybrid and Cyber Security Threats and the EU's Financial System." *Journal of Financial Regulation* 6(2): 180–201. https://doi.org/10.1093/jfr/fjaa006.

Evans, Carol V. 2020. "Future Warfare: Weaponizing Critical Infrastructure." *Parameters* 50(4): 59–70. https://doi.org/10.55540/0031-1723.1017.

Fiott, Daniel, and Roderick Parkes. 2019. *Protecting Europe: The EU's Response to Hybrid Threats*. Luxembourg: Publications Office of the European Union.

Giannopoulos, Georgios, Hanna Smith, and Marianthi Theocharidou. 2021. *The Landscape of Hybrid Threats: A Conceptual Model: Public Version*. Hybrid CoE Research Report. Luxembourg: Publications Office of the European Union.

Hybrid CoE. 2019. *Nuclear Energy and the Current Security Environment in the Era of Hybrid Threats*. Hybrid CoE Research Report. The European Centre of Excellence for Countering Hybrid Threats.

Jokinen, Janne, Magnus Normark, and Michael Fredholm. 2022. *Hybrid Threats from Non-State Actors: A Taxonomy*. Hybrid CoE Research Report 6. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen. 2019. *Hybrid Threats and Vulnerabilities of Modern Critical Infrastructure – Weapons of Mass Disturbance (WMDi)?* Hybrid CoE Working Paper 4. The European Centre of Excellence for Countering Hybrid Threats.

Jukka, Savolainen, Terry Gill, Valentin Schatz, Lauri Ojala, Tadas Jakštas, and Pirjo Kleemola-Juntunen. 2019. *Handbook on Maritime Hybrid Threats: 10 Scenarios and Legal Scans*. Hybrid CoE Working Paper 5. The European Centre of Excellence for Countering Hybrid Threats.

Mazaraki, Nataliia, and Yulia Goncharova. 2022. "Cyber Dimension of Hybrid Wars: Escaping a 'Grey Zone' of International Law to Address Economic Damages." *Baltic Journal of Economic Studies* 8(2): 115–120. https://doi.org/10.30525/2256-0742/2022-8-2-115-120.

Nave, C., V. Kopustinskas, E. Dirginčius, L. Walzer, G. Beniulytė, A. Purvins, M. Masera, D. Nussbaum, V. Norg, and D. Užkuraitis. 2022. *Tabletop Exercise: Coherent Resilience Baltic 2021 (CORE 21-B) Final Report*. Joint Research Centre (JRC) Technical Report. https://doi.org/10.2760/74397.

Schaub, Gary, Martin Murphy, and Frank G. Hoffman. 2017. "Hybrid Maritime Warfare: Building Baltic Resilience." *RUSI Journal* 162(1): 32–40. https://doi.org/10.1080/03071847.2017.1301631.

Tessari, Paola, and Karolina Muti. 2021. *Strategic or Critical Infrastructures, a Way to Interfere in Europe: State of Play and Recommendations*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

Wigell, Mikael, Harri Mikkola, and Tapio Juntunen. 2021. *Best Practices in the Whole-of-Society Approach in Countering Hybrid Threats*. European Parliament/Policy Department for External Relations Study. European Parliament's Think Tank database.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Hafnium and the zero-day dilemma. Public-private cyber threat intelligence cooperation

Mihai OLTEANU*
*Doctoral Studies, "Carol I" National Defense University, Bucharest, Romania
e-mail: mihaiolteanu48@yahoo.com

Abstract

Cyber threat intelligence (CTI) plays a crucial role in limiting cybersecurity risks, with a particular focus on identifying and mitigating zero-day vulnerabilities. While academic literature, specialized reports, and normative documents widely argue in favor of cooperation between public and private entities to develop cybersecurity, significant systemic challenges hinder effective intelligence sharing when discussing real-time threats, such as zero-day vulnerabilities.

This article critically examines the dynamics of public-private collaboration in CTI, focusing on the obstacles preventing further development of the level of cooperation, such as trust deficits, legal constraints, financial and reputational risks, and diverging strategic interests. By performing a qualitative analysis on the existing literature and using the Hafnium cyberattack as a case study, the research highlights the complexities surrounding the zero-day vulnerability disclosures and the limitations of existing cooperative frameworks. The findings indicate that while structured CTI-sharing mechanisms exist, real-time collaboration on zero-day vulnerabilities remains constrained by competing incentives that are unlikely to be properly addressed.

Keywords:

Cyber Threat Intelligence; Hafnium; Zero-day Vulnerabilities; Public-private Cooperation.

Article info

Received: 23 June 2025; Revised: 29 July 2025; Accepted: 26 August 2025; Available online: 6 October 2025

Citation: Olteanu, M. 2025. "Hafnium and the zero-day dilemma. Public-private cyber threat intelligence cooperation." *Bulletin of "Carol I" National Defence University*, 14(3): 328-346. https://doi.org/10.53477/2284-9378-25-52

1. Introduction

Multiple types of cyber threat intelligence reports and studies consistently highlight the increased number of cyber-attacks, which excel both in diversity and technical complexity, that require extensive security measures and force authorities to develop cooperation on any given level, be it state-private, international, internal, inter-institutional, state-academia, and so on. There is a common view that is promoted both in the academic and professional areas, and it states that the ever-evolving cyberthreats require adaptive measures and more cooperation of any kind. This perspective has been around for many years. A study published in 2007 argued the need to develop international cooperation between countries and law enforcement agencies to combat and investigate cybercrime (Cerezo, Lopez and Patel 2007). Further away, in 2002, over two decades ago, Lewis argued in favor of a new normative framework that required international cooperation in cybersecurity, considering the continuously growing interdependence between different systems (Lewis 2002). Back in 1995, there were authors who anticipated that the development of the cyber world would seek new ways for cooperation among people (Rheingold 1994). Today, cybersecurity cooperation is inherent to any strategic or pragmatic document, a very high number of formats being created and operationalized, such as the NATO Cooperative Cyber Defence Centre Of Excellence, a hub focused on research and training (Smeets 2022), or Malware Information Sharing Platform (MISP), a platform focused on sharing cyber threat intelligence reports across multiple actors (Wang, et al. 2024).

Therefore, this emphasis on cooperation is not merely theoretical. In practice, the last two decades have sought to bridge the gap between sectors, nations, and actors, though various initiatives with different levels of commitment. Nonetheless, the outcomes of these efforts—whether successful or unsuccessful—require further analysis. Also, it is unclear if the cooperation mechanisms could be further developed.

The ongoing push towards improving the cyber-related cooperation mechanisms highlights a critical point: the main actors in the cyber sphere (namely, states and firms) have not managed to find a satisfactory approach to this matter. There may be multiple reasons, such as different interests or constraints generated by legal and regulatory hurdles (GDPR on one side, and national security on the other), and concerns over intellectual property (Bechara and Schuch 2020). The whole process of cyber threat intelligence sharing gains a higher urgency when it is narrowed down to exchanging data related to zero-day vulnerabilities, flaws in software or hardware that are exploited before developers have managed to find them and, inherently, release a patch (Singh, Joshi and Kanellopoulos 2019). The impact of exploiting this type of vulnerability is profound, both technically and economically, reducing the trust between the parties at the lowest level, considering that core interests such as the reputation of the company and the security of the states are at stake.

This article examines the fundamental challenges surrounding public-private cooperation in cyber threat intelligence sharing, with a focus on the structural incentives driving both sides—why each chooses to share or withhold data. The analysis will specifically address zero-day vulnerabilities, exploring how these unique threats shape the approach to information sharing and the strategies for mitigating the risks they pose.

2. Methodology

The primary objective of this research is to identify the obstacles to sharing cyber threat intelligence in a public-private context and examine how these barriers affect cooperation on zero-day vulnerabilities. To address this, the research adopts a qualitative approach, analyzing existing literature through technical lenses. Additionally, a case study on the Hafnium zero-day campaign will be presented. This case study: (1) illustrates the need for analyzing the success or failure of actual cooperation mechanisms and (2) provides critical insights into the challenges of the strategies for enhancing cooperation on zero-day vulnerabilities.

3. Cyber threat intelligence and zero-day vulnerabilities

Cyber threat intelligence (CTI) is a component of the larger concept of intelligence, with similar features and final goals (Sülü and Daş 2022). CTI has been defined as a field of activity in which data is collected, compared, analyzed, and, finally, disseminated, aiming to better understand the threats, as well as the threat actors that intend to produce damage to different components of the cyber ecosystem (Sun, et al. 2023). It is also considered to be a process that allows organizations or countries to better understand their vulnerabilities (Shackleford 2015).

The whole CTI process enables organizations to think and act proactively in their attempts to understand the risks and threats, as well as take advantage of the opportunities that occur in cyberspace. Therefore, the *raison d'être* of the CTI is to support the decision of stakeholders on different levels, from cyber commanders of cyber operation units to leaders of the countries and CEOs of private organizations (Lanzendorfer 2015). In doing so, CTI uses all sorts of technical data (e.g., IPs, geolocation, traffic, and so on) to understand the kind of attack that occurred, the mitigation measures required, the capabilities of the threat actor, and the existing vulnerabilities (Barnum 2014). CTI is an activity conducted in an attempt to predict threats by anticipating the attacker's next step and their main objectives, as well as the techniques used to fulfill them in the long run. In that sense, a vital component of the CTI relies on finding the existing vulnerabilities before the attacker does, to prevent their exploitation (Schlette, et al. 2021).

In this context, a particular critical and high-risk category of threats is posed by the zero-day vulnerabilities, which are unknown to the producer and, therefore, silently exploited by threat actors until patches are published (Roumani 2021). The challenge

with zero-days is that these are, by definition, known only by the specialist who found them, meaning that traditional defense mechanisms—such as signature-based detection systems—tend to be ineffective (Ahmad, et al. 2023).

The proactive nature of CTI is particularly important when it comes to zero-day vulnerabilities. Identifying and mitigating these vulnerabilities requires a deep understanding of both the threat landscape and the behavior of threat actors. However, the complexity and lack of knowledge introduce significant challenges for CTI (Albanese, et al. 2013). Unlike other threats, zero-days often require an immediate, coordinated response from both private and public sector organizations, making their timely identification and disclosure essential for minimizing damage.

Given their high value both for the offensive and the defensive sides, the zero-day vulnerabilities have become a source of income for researchers who choose to work on identifying and further commercializing them in white, grey, or black markets. The financial value of a zero-day vulnerability is given by multiple factors, the most important of them being, naturally, its secrecy. For instance, researchers may gain up to $3 million if they choose to sell the zero-day vulnerability on the grey market (Meakins 2018) to customers who are aiming to exploit it in their best interest. Over the last two decades, multiple zero-day vulnerabilities were exploited, some of them producing significant damage, such as Shellshock (on Unix and Linux systems), Heartbleed (Internet disruption), and F5 BIG-IP (HTTP requests that allowed code execution) (Teodorescu 2022). A report published by Google and Mandiant revealed that there were 97 zero-day vulnerabilities identified in 2023, 36 of which targeted enterprise-focused technologies (Google, Mandiant 2024).

4. Cyber threat intelligence cooperation

As stated in the introductory part, the nature of the CTI activity (particularly in relation to zero-day vulnerabilities) constantly underscores the need to create cooperative formats and improve the existing ones, so that cybersecurity threats are adequately prevented and mitigated.

Naturally, the need for cooperation has been argued in numerous academic papers that reflect both quantitative and qualitative benefits that might be achieved through such approaches (Pala and Zhuang 2019). In the case of zero-day vulnerabilities, the challenges could be even more pressing. Since these vulnerabilities are unknown to both vendors and defenders until they are exploited, it is unlikely for a singular organization to possess all the necessary information to respond effectively (Homburger 2019). In the absence of a cooperative public-private format, the ability to swiftly respond to and neutralize these threats is likely to be severely compromised.

The most accessible mechanism of cooperation is exchanging cyber threat intelligence reports, as this directly supports information sharing. Exchanging

technical data such as indicators of compromise, attack vectors, or tactics involved has been acknowledged to be a well-established mechanism for building a collective knowledge related to the cyber threat landscape, allowing for a faster identification of the incident and for adequate measures to be implemented in the aftermath (Wagner, et al. 2019). Similarly, in the case of zero-day vulnerabilities, sharing cyber threat intelligence reports is highly probable to support the efforts of each one of the partners in identifying the flaw and providing a timely patch.

The development of early detection capabilities is a direct result of active cooperation among different actors, as this allows different types of organizations to pool their expertise and resources, hence creating a comprehensive monitoring system. Theoretically, both private and public organizations can provide valuable knowledge that is likely to be complementary in multiple areas. While governments may develop more advanced capabilities in understanding state-sponsored cyberattacks, private companies possess much more real-time data regarding the activity of different categories of threat actors (Purohit, et al. 2023). Therefore, combining these two approaches into cooperative formats should provide the necessary links to better detect and prevent cyberattacks. This goes further in the case of zero-day vulnerabilities, as both actors possess the capabilities to identify this kind of flaw through research and bug bounty programs conducted by their technical experts (Arshad, et al. 2024).

Effective sharing data mechanisms can develop the relationship between states and private companies, further allowing them to build trust and, possibly, develop cooperative formats that create the required context for resource-sharing, allowing them to leverage each other's tools, platforms, and expertise. At least from a defensive standpoint, that approach is entirely desirable, as each of the two parties works towards finding suitable mechanisms to better protect their networks (Rajamäki 2017). That is also completely valid in the case of zero-day vulnerabilities, as public-private bug bounty programs are likely to prove themselves more effective and faster in finding hardware or software vulnerabilities.

Moreover, multiple private-public formats have been established, approaching different configurations and various types of actors, aiming to implement security measures and develop resource-sharing efforts. Each of these collaborative formats provides some added value in the fight against cyber threat actors and cyber vulnerabilities, but it is unknown whether or not the maximum level of cooperation has been reached. Considering that academic literature continues to argue in favor of developing cooperative mechanisms, it is likely that there is more room for cooperation, or at least different entities are advocating so.

Up until now, some of the most common formats of sharing CTI are the Information Sharing and Analysis Centers (ISAC), which have been developed across various industries and encourage sharing data related to cyber threats, Computer Security

Incident Response Teams (CSIRT), as well as different organizational structures and online sharing platforms (Wallis and Leszczyna 2022).

An ISAC is a format designed to facilitate the exchange of information related to cyber threats and threat actors, primarily through voluntary communication between different entities. Typically, an ISAC does not require the sharing of real-time technical data, such as traffic logs or malware samples. Instead, its focus is on raising awareness among its members. ISACs are common in organizations that may not yet have established high levels of trust or are not ready to share critical data (Steffensen and Gnanasekaran 2024).

A more advanced format that has been developed is the CSIRT, a mechanism that commonly uses different types of resources in order to prevent, identify, investigate, and mitigate different types of cyber threats. The entities that join a CSIRT, be they public or private, acknowledge the need to commonly share their resources to prevent cyberattacks from damaging their networks (Bada, et al. 2014). Currently, CSIRT is the most common resource-sharing format, encouraged by multiple bodies, with a special focus coming from the European Union, through the legislative mechanisms among its member states, shaped through the Directive (EU) 2022/2555 (NIS 2 Directive), that highlights the need to create a CSIRT for each of the addressed sectors, coordinated by a chosen authority (not necessarily a public one), with sufficient resources to be able to prevent specific cyber threats (European Parliament, Council of the European Union 2022).

Other agencies, such as the European Union Agency for Cybersecurity (ENISA), were established to provide guidance in handling cyber threats and preventing cyberattacks from occurring (Sklyar and Kharchenko 2019). Although it has been the subject of multiple changes over time (both in terms of structure and objectives) and does not currently hold any technical responsibilities, ENISA still manages to collaborate with private and public entities to create reports that highlight good practices and pieces of advice in the field of cybersecurity (Cavelty and Smeets 2023). ENISA stands out as a useful landmark in public-private cooperation, considering that it is an initiative of the public side. In the private area, multiple platforms have been established, and MISP stands out as being one of the most popular among them. MISP allows its members and volunteers to constantly share technical indicators related to cyber threats, such as indicators of compromise, vulnerabilities, and counter-measures (Wagner, et al. 2016).

While these formats provide various cyber threat intelligence sharing mechanisms and a wide range of options for an actor that is willing to cooperate in mitigating and preventing identified cyberattacks, the existing literature highlights that some impediments are still in place and unlikely to disappear. How these affect the chances of cooperation on multiple threats (and, particularly, on zero-day vulnerabilities) is to be addressed in the following chapters, which aim to highlight some systemic

difficulties in developing a more advanced format of cooperation, or, at least, the one that has been constantly pursued in the last decades. The impact of these matters on handling this type of vulnerability is, naturally, the focus point of this analysis and the role of the study itself.

5. Systemic setbacks in expanding the cooperative formats

While the development of cooperation is theoretically expected (as presented in the previous chapter) and sought by both public and private sector actors (at least on a certain level), and its defensive outcomes and benefits cannot be overlooked, the ideal cooperation format cannot be realized in practice. Numerous financial, social, reputational, and legislative barriers are challenging to overcome and will be addressed in this part of the paper.

A study conducted (Lanzendorfer 2015) on the American perspective regarding the CTI industry and the interaction between public and private entities addressed a set of questions to a group of American officials, and the following conclusions were reached:

- 58.82% of the participants agreed that the expertise of cybersecurity organizations surpasses the US Government's knowledge in the field;
- 70.59% trusted the private contractors to deliver effective products for the US Government in the cyber field;
- 58.82% considered that the private industry possesses more knowledge than the US Government concerning cybersecurity.

While this study does not provide a comprehensive analysis regarding the interaction between public and private organizations, it does raise certain perspectives related to the perception of public entities of the private industry. In this sense, it would be obvious that sharing the result of the CTI activity among as many actors as possible would be the right solution in handling cyberattacks (Fischer, et al. 2023). However, there are numerous reasons observed over the last decades against sharing CTI between different types of entities.

5.1. Lack of trust

One of the most important elements that prevents the day-to-day sharing of CTI is the lack of trust among multiple entities in the spectrum of cyber intelligence.

Firstly, the low level of trust in data exchange between public entities is primarily driven by the operational risks associated with sharing intelligence related to ongoing campaigns. Unlike fields such as counterintelligence or counterterrorism, CTI data is most valuable in real-time, as the real risk lies in the potential expansion of a cyber campaign to additional national entities. When exchanging real-time data between public entities, one must take into account the risk that such sharing could jeopardize ongoing CTI investigations. If another authority starts its own investigation, it could alert the attacker to the exposure. To support this, a study published by CCDCoE

pointed out that there are numerous situations in which even written agreements for information sharing among public organizations are not honored by both parties (Tolga 2019). In this scenario, public entities are more likely to share the relevant data only with a limited number of highly trusted partners or at the point at which their investigations are at least partially completed, and sharing would not produce any additional operational risks or threats.

Secondly, the lack of trust is also a problem in sharing data among private organizations, as there are problems related to open market competition and the risk of losing clients. Private organizations are often reluctant to share their data with competitors operating within the same industry, even when there is potential to enhance client services and prevent cyberattacks from compromising networks. While sharing CTI could help prevent the spread of cyberattacks across various sectors and countries, long-term trust between these organizations is unlikely to develop. This is because their primary focus remains on financial interests, which take precedence over collaborative efforts (Hausken 2007). When private companies operate in different sectors, they are more likely to share real-time data, provided that there is a prior agreement in place and a common financial interest. However, this arrangement does little to advance CTI cooperation, as one party will not operate in the field of cybersecurity and, subsequently, would not own any valuable CTI to share, preventing meaningful exchange.

Thirdly, sharing CTI between private and public entities is challenging from several perspectives. First of all, the process of sharing requires each of them to build a high level of trust, as the government will provide sensitive data to the company, and the private organization will share the investigations conducted at its expense. Additionally, sharing valuable CTI could mean that the government has to provide data about its citizens to a private entity, which might be seen as unacceptable by the general society, given that the company's primary motivation is financial. On the other side, the company might be subject to some regulations that prevent it from sharing its clients' data with third parties that have not been initially agreed upon (Sullivan and Burger 2017).

5.2. Lack of quality

A permanent mechanism of CTI sharing is difficult to establish, as no guarantees of reciprocity may ever be implemented. Some authors underlined that one of the problems related to sharing CTI is that a lot of information is outdated and cannot provide true, valuable insights into ongoing investigations, especially considering that there is a lot of public data and reports, while the analyzing tools and resources require time and effort to provide accurate interpretations (Schlette, Böhm, et al. 2020).

Both public and private actors lack assurance that the information shared will lead to a response that genuinely advances investigative efforts, making the burden of overcoming trust and legislative obstacles seem unjustified in some cases.

Moreover, a standardization mechanism, quality-wise, is difficult and unlikely to be implemented between multiple parties, as each entity holds specific resources and tools when conducting cyber investigations. While this obstacle could potentially be addressed between two parties, cooperative mechanisms involving multiple actors are unlikely to succeed, as no homogenous format could be agreed upon.

5.3. Reputational damage

When sharing CTI, both public entities and private organizations risk exposing themselves to either public criticism or the risk of damaging their reputation. Many organizations that faced a major cyberattack that managed to produce substantial damage to their infrastructure are likely to avoid making their investigation public soon, as there are multiple risks involved: (1) their clients may consider that there was a lack of cybersecurity measures which allowed their data to be endangered and could decide to end the collaboration with the company (Perera, et al. 2022); (2) the private organization may face competitive disadvantages if the information about a cyber campaign goes public, as their rivals will try to prove that they have a higher level of cybersecurity (Lanzendorfer 2015); (3) both private and public organizations may face the risk of being heavily targeted in the near future, as they acknowledge the lack of proper security measures (Kamiya, et al. 2018). Essentially, governments could face similar challenges, as real-time disclosure can fuel public panic and erode trust in their ability to protect critical infrastructure.

These risks, while not inherent to collaboration, underscore why entities often avoid sharing real-time data during a cyberattack. Post-factum threat reports remain a safer alternative, though their value and consistency may still be influenced by the same underlying concerns. Balancing transparency with these risks is a persistent challenge in the evolving landscape of cybersecurity.

5.4. Lack of standardization

Both public and private entities tend to avoid sharing CTI as there is no standardization framework for building the CTI reports, making them difficult to use in the case of a real-time cyber campaign. Different authors argued that the lack of standardization in the CTI industry is making the whole process of sharing data highly ineffective (Silva, et al. 2020), while many of them provide new or innovative formats for standardizing the information sharing (Tounsi and Rais 2017), which, however, were not adopted widely across the industry.

The whole problem related to the lack of standardization is that the efforts of sharing CTI among different public and private organizations and the risks that derive from this process are not worthwhile if there is no guarantee that the outcome will be useful in conducting the cyber investigation and protecting the network (Serrano, Dandurand and Brown 2014). Therefore, as no clear gains are guaranteed, it is burdensome to argue in favor of sharing critical data that is time sensitive and highly valuable, when lacking any incentive related to solving the cybersecurity crisis or limiting the damages.

5.5. Legislative problems

The entire process of sharing CTI is quite difficult, considering that some legislative measures prevent this activity, especially in the case of private organizations sharing their clients' technical data. The General Data Protection Regulation (GDPR) governs activities within the EU and specifically outlines the limitations and conditions for sharing citizens' personal data, which may include cyber-related indicators, such as users' IP addresses (Albakri, Boiten and Lemos 2018). GDPR defines personal data as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data,* ***an online identifier*** *or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*" (European Commission 2016). While GDPR works on safeguarding the data of European citizens, it clearly limits the possibility of sharing with third parties any information that may be labeled as personal data, hence reducing the real-time CTI sharing capabilities.

An extensive investigation on the impact of GDPR on CTI sharing was conducted by Albakri, Boiten, and Lemos, who concluded that companies can exchange personal data related to cyberattacks only with certain public authorities, using encryption mechanisms (Albakri, Boiten and Lemos 2019).

5.6. Different interests

As both public and private entities pursue different endeavors and describe their objectives significantly differently, the real-time CTI cooperation is affected too; some core limitations negatively impact any cooperation format. Typically, private companies prioritize their profits, hence choose to support initiatives that promise returns at least proportionate to their initial investments. Their focus is often on addressing major, high-profile threats that could lead to significant financial losses or reputational damage, such as destructive attacks, espionage or massive cyber-criminal campaigns (Maschmeyer, Deibert and Lindsay 2020). This focus can lead to reluctance in sharing CTI with public entities, as the information related to the "big fish" is highly valuable.

In contrast, governments would choose to prioritize any investigation that could provide real-life added value in society by protecting the majority of the population, as well as organizations and firms of any size. For instance, a "small fish" such as a phishing campaign may seem unattractive to private actors but essential to state authorities, as they may prove to affect a wider part of the population. In that sense, governments are willing to fund investigations that do not seem to be profitable from a financial point of view (Tropina 2015).

This discrepancy in interests – profit-driven motives versus national security objectives – shapes an important barrier in effective cooperation related to CTI.

Meaningful data sharing is less likely to occur in any situation that faces two different perspectives and a separate set of measures. Surely, in the case of a campaign that is of interest to both sides, it is more likely to see a fruitful cooperation, but that type of situation is rather isolated, considering the perspective presented above.

6. Navigating the challenges of disclosing and sharing zero-day vulnerabilities

Although the discussion related to sharing CTI seems pretty straightforward because there is a clear set of benefits as well as some strong risks or disadvantages related to public-private cooperation, that is not the case with exchanging zero-day vulnerabilities, as these tend to be seen differently, considering their value and scarcity.

The advantages of sharing CTI and improving cooperation that were presented in Chapter 4 do not entirely mirror the approach related to zero-day vulnerabilities. Most of the advantages of cooperating rely on post-factum information exchange or preventive collaborative formats in regard to cyberattacks. Therefore, from a defensive point of view, cooperation seems like an adequate recipe. Still, in the case of public-private zero-day exchanges, two main problems arise: (1) on the side of the public entity, why should the authorities freely provide such a valuable vulnerability to a private entity, sacrificing its secrecy against its own interest? (Bilge and Dumitraș 2012) and (2) on the side of the company, why should it share the zero-day and risk of having it exploited instead of patching it? The whole debate seems like a zero-sum game, in which neither of the actors has clear reasons to believe that both players will win. The entire list of advantages used by different entities to promote CTI sharing is not valid in case of a singular vulnerability, most likely unknown by any other actor that could provide significant strategic advantages. No level of trust can compensate for sharing such an important asset with an actor that, as explained previously, has different views and objectives.

Moreover, on the side of the private entity, there is another essential question, namely: with whom to share the zero-day vulnerability? While the public-private discussion seems to refer to two actors, in reality, the number is significantly higher. The great companies conduct their cybersecurity operations and commercialize their products in a large number of states, meaning that a fair cooperative initiative would require them to announce all of their partners (namely, all of the different states) that it has found such a zero-day vulnerability and expect them to act rightfully. That oversteps any financial interest and business strategy, as the value of the asset will significantly drop, while also risking its exploitation (Roumani 2021).
Besides, the reputational damage of the company is still in place, considering that sharing such an important flaw in their hardware or software product with the risk of it going publicly might significantly affect the trust of the customers and, furthermore, its financial interests in the long run (Ekong, et al. 2023).

Another problem that arises from the argument exposed in the 5.2 chapter is that of quality and reciprocity. It is difficult (if not impossible) to build the required trust mechanisms that would work in such a way that either the public authority or the private actor would have the confidence that a mirrored situation would produce a similar outcome (Schulze and Reinhold 2018) and, conclusively, decide to share a newly found zero-day vulnerability.

More progress could be made on the side of public authorities, especially states that are part of common organizations. The European Union tries to encourage the efforts towards programs of Common Vulnerability Disclosure, as this is a part of the NIS2 Directive, that regulated some mechanisms to protect the researcher that identified the vulnerability, and encourages member states to share their findings inside the EU, then with the private entity and, finally, publicly, when a patch has been developed (European Parliament, Council of the European Union 2022). Still, it is unlikely that a similar approach would be adopted on the side of private companies, which are likely to maintain the status quo, which consists of identifying zero-days and only sharing them (with partners, or publicly) when the proper security update has been created and tested.

7. Hafnium: Case Study on the Exploitation of Zero-Day Vulnerabilities

The Hafnium cyberattack, first identified at the beginning of 2021, represents one of the most significant and widespread security breaches in recent history, based on zero-day vulnerabilities. The campaign was publicly attributed to a China-based advanced persistent threat group (NATO 2021) and consisted of exploiting vulnerabilities in Microsoft Exchange Servers, managing to produce a significant impact worldwide. The cyber threat actors successfully gained unauthorized access to systems and email servers, stole sensitive data, and deployed advanced malware that could be exploited for a long period of time (Waheed, et al. 2024).

The campaign was based on the complementary exploitation of four zero-day vulnerabilities found by Chinese hackers and used for several months in a row. The zero-day vulnerabilities allowed the attacker to:

- Authenticate to the Microsoft Exchange servers that allowed stealing the content of the mailboxes through CVE-2021-26855 (Server-Side Request Forgery);
- Gain access to voice mail functionality, if administrator privileges are previously obtained, through CVE-2021-26858 (Insecure Deserialization);
- Write files (potentially malicious ones) on the compromised servers through CVE-2021-26858 and CVE-2021-27065 (Arbitrary File Write) (Narang 2021).

There are different estimations on the global damage that was produced, but several public sources claim that the Hafnium campaign managed to compromise between

10.000 and 250.000 Microsoft customers, including businesses and governmental agencies. Moreover, Microsoft inflicted severe reputational damage after this cyberattack that was based on vulnerabilities, with US-China relations also estimated to be affected (Bates 2022).

On the 2nd of March 2021, Microsoft published a communication entitled "New nation-state cyberattacks" describing the cyber threat actor dubbed Hafnium, as well as the fact that it exploited some "previously undiscovered vulnerabilities" in the products commercialized by the American company. It also stated that it briefed the U.S. government about the incident and that it was helped by other companies to address the vulnerabilities (Burt 2021). This was the first moment in which Microsoft acknowledged the existence of zero-day vulnerabilities and their exploitation. On the same day, it publicly released some patches to address these vulnerabilities, which were then updated constantly to prevent any further damages (Microsoft 365 Security 2021).

Different public sources point out that Microsoft was warned about the vulnerabilities at least two times, by different cybersecurity companies, since January 2021. Initially, Volexity saw the attackers quietly exploiting the zero-day vulnerabilities and communicated this to Microsoft. In February, before the official acknowledgment made by Microsoft, Volexity saw massive exploitation of the same vulnerabilities (Krebs 2021). Moreover, at least one more private entity told Microsoft about the active exploitation of the zero-day vulnerabilities in January 2021 (Robinson 2024).

7.1. What did Hafnium highlight?

After looking into the specifics of the Hafnium case, some ideas may be outlined in support of the points previously made regarding the cooperation on the zero-day cybersecurity vulnerabilities.

Q: Did Microsoft share the insight on the existing zero-day vulnerabilities?
A: Yes, but only after it developed a security patch. As pointed out in Chapter 6, although there were several pieces of evidence that pointed out that Microsoft was aware of the zero-day vulnerabilities before going public and sharing the insights, it chose to do so only when a patch had been developed. In doing so, it proved that its interest was, first of all, reputational (and, therefore, financial) because Microsoft chose to maintain the secrecy about the actively exploited vulnerabilities in an attempt to, most likely, avoid losing clients by admitting the problems without having a practical solution. For the general victims, it is likely that a public statement made before the 2nd of March would have been more helpful in implementing mitigation measures and, conclusively, limiting the number of compromised servers. However, Microsoft acted in its own interests, namely, protecting its financial objectives.

Q: Was there active cooperation between private actors?
A: Yes and no. On one side, multiple private entities, such as Volexity, chose to

cooperate by informing Microsoft about the zero-days, but only because they could not exploit them in their own interests; therefore, they did not compete in this matter. On the other side, Microsoft's communication from the 2nd of March did not include any form of cooperation in developing the patches with other private cybersecurity companies, although it is likely that the update would have been developed earlier. One possible reason could be that a cooperative approach would force Microsoft to admit that it was unable to single-handedly deal with the zero-days and needed to cooperate with a competitor.

Q: Was there active cooperation between public and private actors?
A: No. While Microsoft knew about the vulnerabilities, it only chose to brief the US government, while all the other states that use its technology were unaware of the zero-days. As pointed out in Chapter 6, sharing this kind of data in real-time with all the public authorities is unlikely, as it is not in the company's best interest. Therefore, governmental networks were compromised, as no state other than the US was able to implement preventive measures.

Q: Was there active cooperation between public actors?
A: It is unknown. There is no public evidence that any other state, besides the US, knew about the Hafnium campaign. Moreover, the high number of victims worldwide could underline that states were not able to implement timely defensive measures.

Conclusions

This analysis, directly supported by the Hafnium case study, highlights the obstacles in sharing zero-day vulnerabilities between all sorts of actors. While such cooperation could provide more timely measures (as the Hafnium campaign highlights), the main arguments behind this situation are systemic and unlikely to be overcome in the long run. The fundamental difference in the core interests of the states and private companies converges to a lack of extensive cooperation in dealing with real-time data, specifically focused on zero-day vulnerabilities.

Although several formats try to address this matter, their success is questionable, as well as their improvement perspectives. Volexity proves that a certain amount of cooperation is definitely possible when non-competitive interests are in place. Microsoft demonstrated that proactively cooperating with partners and promoting its financial interests are two mutually exclusive approaches. The fundamental misalignment of incentives between public and private actors indicates that a fully cooperative cybersecurity model remains difficult to achieve. While initiatives like public-private partnerships and information-sharing platforms provide some progress, they do not fully address the deeper systemic issues that have been presented in the previous chapters.

However, the active real-time cooperation between Microsoft and the US government in regard to Hafnium needs to be studied, as it creates the premises of a situation in which it seems that the company overstepped its financial interest and cooperated with an official body.

References

Ahmad, Rasheed, Izzat Alsmadi, Wasim Alhamdani, and Lo'ai Tawalbeh. 2023. "Zero-day attack detection: a systematic literature review." *Artif Intell Rev* 10733–10811. https://doi.org/10.1007/s10462-023-10437-z.

Albakri, Adham, Eerke Boiten, and Rogério De Lemos. 2018. "Risks of Sharing Cyber Incident Information." *Proceedings of the 13th International Conference on Availability, Reliability and Security* 1-10. https://doi.org/10.1145/3230833.3233284.

—. 2019. "Sharing Cyber Threat Intelligence Under the General Data Protection Regulation." *Privacy Technologies and Policy 7th Annual Privacy Forum, APF 2019.* Rome, Italy: Springer. 28-41. https://doi.org/10.1007/978-3-030-21752-5_3.

Albanese, Massimiliano, Sushil Jajodia, Anoop Singhal, and Lingyu Wang. 2013. "An efficient approach to assessing the risk of zero-day vulnerabilities." *International Conference on Security and Cryptography (SECRYPT).* Reykjavik, Iceland: IEEE. 1-12.

Arshad, Junaid, Muhammad Talha, Bilal Saleem, Zoha Shah, Huzaifa Zaman, and Zia Muhammad. 2024. "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry." *Blockchains* 2 (3): 195-216. https://doi.org/10.3390/blockchains2030010.

Bada, Maria, Michael Goldsmith, Chris Mitchell, and Elizabeth Phillips. 2014. "Improving the Effectiveness of CSIRTs." *Global Cyber Security Capacity Centre.*

Barnum, Sean. 2014. *Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™).* The MITRE Corporation.

Bates, Alicia. 2022. "Prepare and Prevent, Don't Repair and Repent." *The Cyber Defense Review* 7 (3): 17-30.

Bechara, Fabio Ramazzini, and Samara Bueno Schuch. 2020. "Cybersecurity and global regulatory challenges." *Journal of Financial Crime* 359-374. https://doi.org/10.1108/JFC-07-2020-0149.

Bilge, Leyla, and Tudor Dumitraş. 2012. "Before we knew it: an empirical study of zero-day attacks in the real world." *CCS '12: Proceedings of the 2012 ACM conference on Computer and Communications Security.* North Carolina, Raleigh, USA. 833 - 844. https://doi.org/10.1145/2382196.2382284.

Burt, Tom. 2021. *New nation-state cyberattacks.* March 02. https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/.

Cavelty, Myriam Dunn, and Max Smeets. 2023. "Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority." *Journal of European Public Policy* 30 (7): 1330-1352. https://doi.org/10.1080/13501763.2023.2173274.

Cerezo, Ana I., Javier Lopez, and Ahmed Patel. 2007. "International Cooperation to Fight Transnational Cybercrime." *Second International Workshop on Digital Forensics and Incident Analysis (WDFIA 2007).* Karlovassi, Greece: IEEE. doi:10.1109/WDFIA.2007.4299369.

Ekong, Anietie P., Aniebiet Etuk, Saviour Inyang, and Mary Ekere-obong. 2023. "Securing Against Zero-Day Attacks: A Machine Learning Approach for Classification and Organizations' Perception of Its Impact." *Journal of Information Systems and Informatics* 5 (3): 1123-1140. doi:10.51519/journalisi.v5i3.546.

European Commission. 2016. *Consolidated text: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* May 04. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504&qid=1532348683434.

European Parliament; Council of the European Union. 2022. "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL." *Official Journal of the European Union.* December 14. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2555.

Fischer, Daniel, Clemens Sauerwein, Martin Werchan, and Dirk Stelzer. 2023. "An Exploratory Study on the Use of Threat Intelligence Sharing Platforms in Germany, Austria, and Switzerland." *ARES '23: Proceedings of the 18th International Conference on Availability, Reliability and Security.* New YorkNYUnited States: Association for Computing Machinery. 1-7. https://doi.org/10.1145/3600160.3600185.

Google; Mandiant. 2024. *We're All in this Together. A Year in Review of Zero-Days Exploited In-the-Wild in 2023.* March. https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf.

Hausken, Kjell. 2007. "Information sharing among firms and cyber attacks." *Journal of Accounting and Public Policy* 26 (6): 639-688. https://doi.org/10.1016/j.jaccpubpol.2007.10.001.

Homburger, Zine. 2019. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace." *Global Society* 33 (2): 224-242. https://doi.org/10.1080/13600826.2019.1569502.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz. 2018. "What is the Impact of Successful Cyberattacks on Target Firms?" *National Bureau of Economic Research.* doi:10.3386/w24409.

Krebs, Brian. 2021. *At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software.* March 05. https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/.

Lanzendorfer, Quinn E. 2015. *Enabling knowledge in the paradigm of international cyber intelligence.* Robert Morris University ProQuest Dissertations Publishing.

Lewis, James A. 2002. "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." *Center for Strategic and International Studies.*

Maschmeyer, Lennart, Ronald J. Deibert, and Jon R. Lindsay. 2020. "A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society." *Journal of Information Technology & Politics* 18 (1): 1-20. https://doi.org/10.1080/19331681.2020.1776658.

Meakins, Joss. 2018. "A zero-sum game: the zero-day market in 2018." *Journal of Cyber Policy* 60-71. doi:10.1080/23738871.2018.1546883.

Microsoft 365 Security. 2021. *HAFNIUM targeting Exchange Servers with 0-day exploits.* March 02. https://www.microsoft.com/en-us/security/blog/2021/03/02/hafnium-targeting-exchange-servers/.

Narang, Satnam. 2021. *CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065: Four Zero-Day Vulnerabilities in Microsoft Exchange Server Exploited in the Wild.* March 2. https://www.tenable.com/blog/cve-2021-26855-cve-2021-26857-cve-2021-26858-cve-2021-27065-four-microsoft-exchange-server-zero-day-vulnerabilities.

NATO. 2021. *Statement by the North Atlantic Council in solidarity with those affected by recent malicious cyber activities including the Microsoft Exchange Server compromise.* July 19. https://www.nato.int/cps/en/natohq/news_185863.htm.

Pala, Ali, and Jun Zhuang. 2019. "Information Sharing in Cybersecurity: A Review." *Decision Analysis* 16 (3): 172-196. https://doi.org/10.1287/deca.2018.0387.

Perera, Srinath, Xiaohua Jin, Alana Maurushat, and De-Graft Joe Opoku. 2022. "Factors Affecting Reputational Damage to Organisations Due to Cyberattacks." *Informatics* 9 (28). https://doi.org/10.3390/informatics9010028.

Purohit, Soumya, Roshan Neupane, Naga Ramya Bhamidipati, Varsha Vakkavanthula, Songjie Wang, and Matthew Rockey. 2023. "Cyber Threat Intelligence Sharing for Co-Operative Defense in Multi-Domain Entities." *IEEE Transactions on Dependable and Secure Computing* 20 (5): 4273-4290. doi:10.1109/TDSC.2022.3214423.

Rajamäki, Jyri. 2017. "Cyber Security, Trust-Building, and Trust-Management: As Tools for Multi-agency Cooperation Within the Functions Vital to Society." In *Cyber-Physical Security. Protecting Critical Infrastructure at the State and Local Level*, by Robert M. Clark and Simon Hakim, 233–249. Springer.

Rheingold, Howard. 1994. *The Virtual Community: Finding Connection in a Computerized World.* Secker & Warburg.

Robinson, Philip. 2024. *The Hafnium Breach – Microsoft Exchange Server Attack.* December 17. https://www.lepide.com/blog/the-hafnium-breach-microsoft-exchange-server-attack/.

Roumani, Yaman. 2021. "Patching zero-day vulnerabilities: an empirical analysis." *Journal of Cybersecurity* 7 (1). https://doi.org/10.1093/cybsec/tyab023.

Schlette, Daniel, Fabian Böhm, Marco Caselli, and Günther Pernul. 2021. "Measuring and visualizing cyber threat intelligence quality." *International Journal of Information Security* 21–38. https://doi.org/10.1007/s10207-020-00490-y.

Schulze, Matthias, and Thomas Reinhold. 2018. "Wannacry about the tragedy of the commons? Game-theory and the failure of global vulnerability disclosure." *ECCWS 2018 17th European Conference on Cyber Warfare and Security V2.* Oslo, Norway: Academic Conferences and Publishing International Limited. 454-463.

Serrano, Oscar, Luc Dandurand, and Sarah Brown. 2014. "On the design of a cyber security data sharing system." *Proceedings of the 2014 ACM workshop on information sharing & collaborative security.* New York, United States: Association for Computing Machinery. 62-69. https://doi.org/10.1145/2663876.2663882.

Shackleford, Dave. 2015. "Who's Using Cyberthreat Intelligence and How?" February. https://cdn-cybersecurity.att.com/docs/SANS-Cyber-Threat-Intelligence-Survey-2015.pdf.

Silva, Alessandra de Melo e, João José Costa Gondim, Robson de Oliveira Albuquerque, and Luis Javier García Villalba. 2020. "A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence." *Future Internet.*

Singh, Umesh Kumar, Chanchala Joshi, and Dimitris Kanellopoulos. 2019. "A framework for zero-day vulnerabilities detection and prioritization." *Journal of Information Security and Applications* 164-172. https://doi.org/10.1016/j.jisa.2019.03.011.

Sklyar, Vladimir, and Vyacheslav Kharchenko. 2019. "ENISA Documents in Cybersecurity Assurance for Industry 4.0: IIoT Threats and Attacks Scenarios." *IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications.* Metz, France: IEEE. doi:10.1109/IDAACS.2019.8924452.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon).* Tallinn, Estonia: IEEE. doi:10.23919/CyCon55549.2022.9811018.

Steffensen, Vilja, and Vahiny Gnanasekaran. 2024. "Information Sharing between the Computer Security Incident Response Team and its Members: An Empirical Study." *NIKT* 3.

Sullivan, Clare, and Eric Burger. 2017. ""In the public interest": The privacy implications of international business-to-business sharing of cyber-threat intelligence." *Computer Law & Security Review* 33 (1): 14-29. https://doi.org/10.1016/j.clsr.2016.11.015.

Sülü, Mücahit, and Resul Daş. 2022. "Graph Visualization of Cyber Threat Intelligence Data for Analysis of Cyber Attacks." *BALKAN JOURNAL OF ELECTRICAL & COMPUTER ENGINEERING.* https://doi.org/10.17694/bajece.1090145.

Sun, Nan, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, and Yonghang Tai. 2023. "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives." *IEEE Communications Surveys & Tutorials* 25 (3): 1748-1774. doi:10.1109/COMST.2023.3273282.

Teodorescu, Cosmin Alexandru. 2022. "Perspectives and Reviews in the Development and Evolution of the Zero-Day Attacks." *Informatica Economică* 26 (2). doi:10.24818/issn14531305/26.2.2022.05.

Tolga, İhsan Burak. 2019. *Whole-of-Government Cyber Information Sharing.* Talinn: CCDCoE.

Tounsi, Wiem, and Helmi Rais. 2017. "A Survey on Technical Threat Intelligence in the Age of Sophisticated Cyber Attacks." *Computers & Security* 212-233.

Tropina, Tatiana. 2015. "Public–Private Collaboration: Cybercrime, Cybersecurity and National Security. In: Self- and Co-regulation in Cybercrime, Cybersecurity and National Security." *SpringerBriefs in Cybersecurity* 1-41. https://doi.org/10.1007/978-3-319-16447-2_1.

Wagner, Cynthia, Alexandre Dulaunoy, Gérard Wagener, and Andras Iklody. 2016. "MISP: The Design and Implementation of a Collaborative Threat Intelligence Sharing Platform." *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security.* Vienna, Austria: Association for Computing Machinery. 49-56. https://doi.org/10.1145/2994539.2994542.

Wagner, Thomas D., Khaled Mahbub, Esther Palomar, and Ali E. Abdallah. 2019. "Cyber threat intelligence sharing: Survey and research directions." *Computers & Security* 87. https://doi.org/10.1016/j.cose.2019.101589.

Waheed, Azheen, Bhavish Seegolam, Mohammad Faizaan Jowaheer, Chloe Lai Xin Sze, and Ethan Teo Feng Hua. 2024. "Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure." *Preprints.* doi: 10.20944/preprints202407.2338.v1.

Wallis, Tania, and Rafał Leszczyna. 2022. "EE-ISAC—Practical Cybersecurity Solution for the Energy Sector." *Energies* 15 (6). doi:https://doi.org/10.3390/en15062170.

Wang, Han, Alfonso Iacovazzi, Seonghyun Kim, and Shahid Raza. 2024. "CLEVER: Crafting Intelligent MISP for Cyber Threat Intelligence." *2024 IEEE 49th Conference on Local Computer Networks (LCN).* Normandy, France: IEEE. doi:10.1109/LCN60385.2024.10639749.

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

Romania's Contribution to the Military Capabilities Developed through the Projects of the European Union's Permanent Structured Cooperation

Maj. Assoc. Prof. Marius PRICOPI, PhD*
*"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania
e-mail: pricopi.marius@armyacademy.ro
https://orcid.org/0009-0008-1869-7084

Abstract

The Permanent Structured Cooperation is a successful initiative through which the European Union develops military capabilities necessary for strengthening the European dimension of security and defence. Using the case study as a scientific method, the present paper examines Romania's level of involvement in the projects conducted within the institutional framework provided by this Permanent Structured Cooperation. By contributing to a significant number of such projects, Romania clearly demonstrates its capacity to operate in a complex international format and to actively collaborate with a large number of participating states, supporting in this manner the strengthening of the European Union's Common Security and Defence Policy. The active participation and, in some cases, even the coordination of such projects, highlight both the cumulated level of professionalism and the expertise of the Romanian state, which, through involvement in these initiatives, contributes directly to generating added value in the area of European defence and security.

Keywords:
Permanent Structured Cooperation; Common Security and Defence Policy; Project; Romania; European Union.

Article info
Received: 10 July 2025; Revised: 29 August 2025; Accepted: 10 September 2025; Available online: 6 October 2025

Citation: Pricopi, M. 2025. "Romania's Contribution to the Military Capabilities Developed through the Projects of the European Union's Permanent Structured Cooperation." *Bulletin of "Carol I" National Defence University* 14(3): 347-354. https://doi.org/10.53477/2284-9378-25-53

In an international context marked by significant changes, the Permanent Structured Cooperation (PESCO) represents one of the main instruments of cooperation available to the European Union (EU) for strengthening its Common Security and Defence Policy. Based on the provisions of Article 42(6) and Article 46 of the Treaty on European Union (European Union 2025), PESCO is actually one of the initiatives undertaken in the process of strengthening the strategic autonomy of the European Union, alongside the European Defence Fund, the Capability Development Plan and the Coordinated Annual Review on Defence (European Defence Agency 2025).

In this institutional framework, there are currently in conduct no less than 75 projects to develop European military capabilities, with the voluntary participation of 26 out of the 27 EU member states (Malta being the only exception) (Permanent Structured Cooperation 2025a). The most popular projects even benefit from the involvement of third states, such as Canada, Norway, and the United States (Permanent Structured Cooperation 2025b).
Although PESCO receives considerable attention in the academic literature, the dimension of Romania's involvement should also be explored. Consequently, the present paper aims to bring additional knowledge on how Romania contributes to the acquisition of military capabilities through the Permanent Structured Cooperation.

Scientific Literature Review

Ever since its formal establishment in December 2017, the Permanent Structured Cooperation has benefited from a significant scientific interest. The academic literature reflects two main research directions: the first focuses on the institutional and regulatory framework of PESCO; the second examines the significantly different involvement of member states in PESCO projects (depending on their availability, possibilities, interests, and priorities).

Thus, regarding the first research direction, it is worth mentioning Sven Biscop's paper (Biscop 2020), as it analyzes how the legal framework and implementation means of PESCO prove sufficient for achieving its initial goals; at the same time, Biscop offers recommendations for optimizing PESCO, such as: focusing on a more specific objective, prioritizing strategically relevant projects, or establishing clear procedures for fulfilling the commitments taken on by participating states. Then, a paper published by Lorenzo Giuglietti at the College of Europe (Giuglietti 2021) makes the case for the potential of PESCO to facilitate transatlantic cooperation, to strengthen the European defence industry, and to promote improved relations with the North Atlantic Alliance. In a scientific paper written by Benjamin Martill and Carmen Gebhard (Martill and Gebhard 2023), the authors demonstrate how the concept of "combined differentiation" has basically become a response to the particularities of the European defence environment; furthermore, they analyze how this differentiation has evolved over time.

Regarding the second research direction, the work of Karolina Gawron-Tabor and Rafal Willa (Gawron-Tabor and Willa 2023) stands out, making a comparative analysis of the involvement of EU member states in PESCO projects; also, the authors identify a series of factors that influence the level of involvement of the countries (such as the regional situation of each state or other political, historical or geographical factors) and analyse some of the issues that could hinder a more significant military cooperation between these countries. In a scientific paper written by Eva Michaels and Monika Sus (Michaels and Sus 2024), it is argued that, although significant progress has been made, there are still some differences between the national perceptions, approaches, and objectives of the member states concerning the security and defence of the European Union.

Regarding the national academic literature, it is worth mentioning the paper published by Ion Anghel (Anghel 2019), which also addresses Romania's involvement in PESCO projects; according to the author, this involvement in relevant projects, within a multiannual financial framework, will contribute to the development of a national vision in the area of international cooperation. The topic of PESCO is also discussed in a scientific paper by Dragoș Ilinca (Ilinca 2022); the author highlights the evolution of PESCO towards a cooperation platform for the development of defence capabilities that thus supports the improvement of the European Union's security and defence profile.

Scientific Methodology

In writing this paper, the scientific methodology of the case study was used, as detailed in the book titled "Doing Case Study Research" (Hancock, Algozzine, and Lim 2021). Relevant quantitative data have been processed and utilised, and afterwards, these were analyzed through the statistical method (minimum value, maximum value, average, median, distributions, and variations).

Thus, the research question is the following: What is Romania's involvement in the development of the European Union's military capabilities (through the framework provided by the Permanent Structured Cooperation)?
Linked with the research question, the scientific hypothesis is as follows: There is a positive correlation between the level of Romania's specialized and significant military contribution to the development of European military capabilities and the strengthening of its national profile within the Common Security and Defence Policy.

Results and Discussion

According to data published on the official PESCO website (Permanent Structured Cooperation 2025b), Romania is currently involved in 18 PESCO projects, out of a total of 75 (Table no. 1). It is indeed a performance, considering that some EU member states are involved in only 3 PESCO projects (as is the case with Denmark

or Slovakia); on the other hand, the biggest contributors to these initiatives are France (49 projects), Italy (40 projects) and Germany (33 projects).

TABLE NO. 1

The involvement of Romania and the other EU member states in PESCO projects

Indicator	Value	Observations
The minimum number of PESCO projects in which some EU member states are involved	3	Denmark, Slovakia
The maximum number of PESCO projects in which a certain EU member state is involved	49	France
The number of PESCO projects in which Romania is involved	18	Position 7 out of 26 EU member states participating in PESCO
The average of EU member states involvement in the PESCO projects	14,76	The value obtained by Romania is 21,95% higher than the average
The median of EU member states involvement in the PESCO projects	12	The value obtained by Romania is 50% higher than the median

Source: Analysis conducted by the author, based on data available on the official PESCO website (Permanent Structured Cooperation 2025b)

As shown in Table no. 1, on average, EU member states are involved in approximately 14,76 PESCO projects; but considering the major differences that exist in this matter between participating countries, more useful than the average is the median of these involvements, whose value is 12. Thus, the value obtained by Romania is higher than both the average (by 21,95%) and the median (by 50%).

Another observation is that among the 18 projects in which Romania is involved, there are also the 2 that benefit from the highest recognition and support within PESCO; the first is the project "Network of Logistic Hubs in Europe and Support to Operations", which benefits from the participation of 20 states, including Canada, and is coordinated by Cyprus, France, and Germany; the second is the project "Military Mobility", in which no less than 28 states participate, including Canada, Norway and the United States, and which is coordinated by the Netherlands (Permanent Structured Cooperation 2025b).

Other observations also emerge from the classification by areas of cooperation of the 18 PESCO projects in which Romania is involved (Figure 1). To respect coherence and methodological rigor, the 7 areas used in the classification are those mentioned on the official PESCO website (Permanent Structured Cooperation 2025b). Likewise, alongside Romania's involvement, the figure also highlights a balanced involvement, understood as a hypothetical equal distribution of the 18 projects across the 7 areas (with a resulting average of 2,57 projects per area).

Thus, out of the 18 projects, Romania is involved in 6 projects that belong to the "Strategic Enablers and Force Multipliers" area. The presence in these initiatives

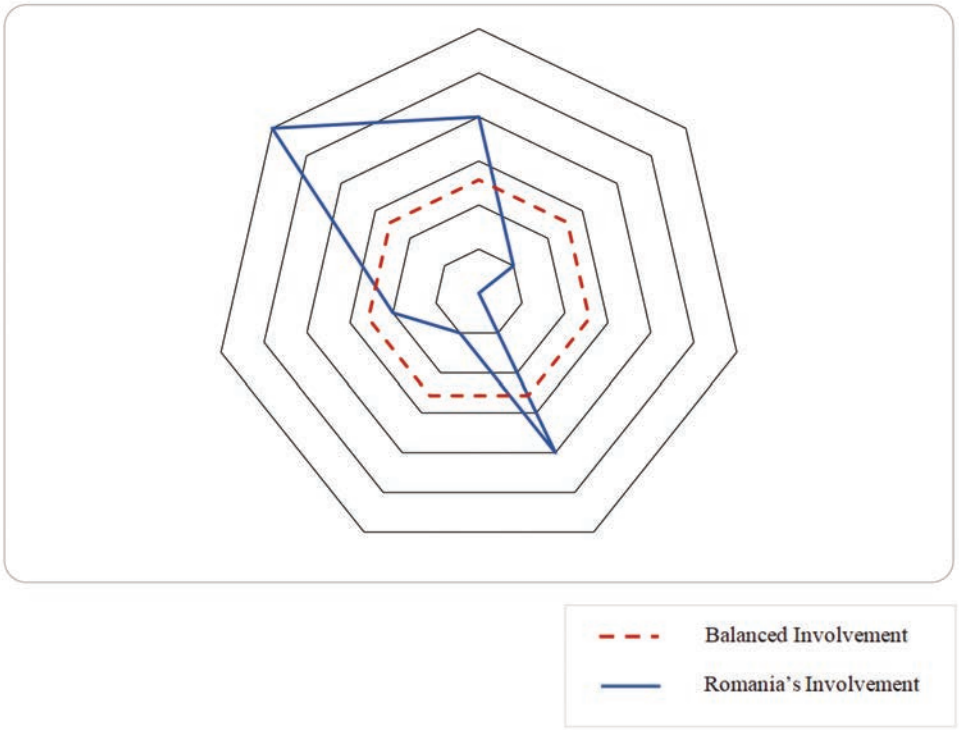

Figure 1 Classification by areas of cooperation of the PESCO projects in which Romania is involved
Source: Analysis conducted by the author, based on data available on the official PESCO website (Permanent Structured Cooperation 2025b)

(aimed to support and enhance already existing military capabilities) reflects the significant role held by Romania, as a state located on the Eastern border of the European Union (and the North Atlantic Alliance); the Romanian state thus demonstrates that it actively takes on both the opportunities and the challenges that result from its geostrategic position.

Another priority for Romania is the "Training, Facilities" area, in which it is involved in 4 projects. Thus, the Romanian state contributes to various initiatives for the common training of the armed forces belonging to the participating states, enhancing their level of interoperability; at the same time, Romania participates in the development of military facilities that enable training at high standards.
The "Maritime" area also receives a similar attention, with Romania contributing to 4 projects as well; the country's geostrategic position at the Black Sea, important for the regional and European security, is thus reflected.

Also, Romania's involvement in the 2 projects regarding the "Space" area (an emerging area for the Romanian state) is commendable and should be encouraged.
But Romania's performance is unbalanced by the reduced participation in the other 3 areas, marking a single presence in the "Cyber", respectively "Air" areas, and no presence in the "Land" area.

Then, as shown in Table 2, Romania coordinates only 2 of the 18 PESCO projects in which it is involved. It is a relative performance, considering the fact that a group of 7 EU member states do not coordinate any projects; on the other hand, France coordinates 17 projects, and Germany and Italy each coordinate 14 projects (Permanent Structured Cooperation 2025b).

TABLE NO. 2

The coordination by Romania and the other EU member states of PESCO projects

Indicator	Value	Observations
The minimum number of PESCO projects coordinated by some EU member states	0	Croatia, Denmark, Ireland, Latvia, Luxembourg, Slovakia, Slovenia
The maximum number of PESCO projects coordinated by a certain EU member state	17	France
The number of PESCO projects coordinated by Romania	2	Position 7 (alongside Finland) out of 26 EU member states participating in PESCO.
The average coordination by EU member states of PESCO projects	2.96	The value obtained by Romania is 32.43% lower than the average
The median of coordinations by EU member states of PESCO projects	1	The value obtained by Romania is 100% higher than the median

Source: Analysis conducted by the author, based on data available on the official PESCO website (Permanent Structured Cooperation 2025b)

According to Table No. 2, on average, EU member states coordinate approximately 2.96 PESCO projects; the value of 2 obtained by Romania is 32.43% lower than the average; again, though, the significant differences among countries make it more useful to highlight the median of these coordinations, whose value is 1. Thus, the value obtained by Romania is 100% higher than the median value.
For example, the first project coordinated by Romania is called "CBRN Defence Training Range", in the "Training, Facilities" area. The project aims to increase the level of interoperability between participating countries with regard to Chemical, Biological, Radiological and Nuclear (CBRN) defence, through individual and collective training (Permanent Structured Cooperation 2025c).

The second project coordinated by Romania is called "European Union Network of Diving Centres", belonging to the same "Training, Facilities" area. This project aims to facilitate the training and certification of divers from participating states, thereby improving the interoperability, deployability, and flexibility of these types of structures (Permanent Structured Cooperation 2025d).

Conclusions

The Permanent Structured Cooperation remains one of the pillars of the European Union's Common Security and Defence Policy. Through PESCO, participating states work together to develop European military capabilities.

The portfolio of PESCO projects of the Romanian state is a diversified one, practically covering 6 out of the 7 specific cooperation areas. This fact indicates a comprehensive approach to defence and Romania's interest in contributing to the development of military capabilities across multiple levels. Moreover, through active involvement in PESCO projects, Romania contributes to increasing interoperability between the armed forces of participating states, at the same time enhancing both the European Union's strategic autonomy and its deterrence and defence capacity.

Additionally, the high degree of specialization existing in the 2 projects coordinated by Romania is also noteworthy. By participating in such niche projects, Romania proves itself capable of bringing added value in those areas where it holds a proven expertise. Such an approach allows Romania to maximize its contribution and its positive impact within the European cooperation in the defence area.

In order to maintain its profile visible and relevant within the Common Security and Defence Policy, Romania has to maintain an active and collaborative approach within the institutional framework established through the Permanent Structured Cooperation. Yet, this fact involves not only participation in existing projects for developing military capabilities, but also the coordination by Romania of a larger number of such projects.

Finally, considering all the data and arguments presented, it can be concluded that the scientific hypothesis of this paper has been validated, and the answer to the research question initially formulated has been provided.
In perspective, the following directions of scientific research could prove useful for future efforts to deepen the understanding of this topic: identifying new PESCO projects in which the Romanian state could get involved (as a participant, or preferably as a coordinator); analyzing the correlation between a more balanced distribution across areas of cooperation of the PESCO projects in which Romania could get involved at the European Union level, on the one hand, and the national interests and strategic priorities of the Romanian state, on the other.

References

Anghel, Ion. 2019. "Cooperation Actions in PESCO Framework". *Proceedings. International Scientific Conference Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, vol. 2: 139-146. https://cssas.unap.ro/en/pdf_books/conference_2019_vol2.pdf.

Biscop, Sven. 2020. "European Defence and PESCO: Don't Waste the Chance". https://www.iai.it/sites/default/files/euidea_pp_1.pdf.

European Defence Agency. 2025. "EU Defence Initiatives". https://eda.europa.eu/what-we-do/EU-defence-initiatives.

European Union. 2025. "EUR-Lex". https://eur-lex.europa.eu/homepage.html.

Gawron-Tabor, Karolina and Rafal Willa. 2023. "Involvement of EU Member States in PESCO Projects: A Comparative Analysis". *Athenaeum. Polish Political Science Studies*, vol. 79 (3): 21-46. 2023. https://bibliotekanauki.pl/articles/22425266.

Giuglietti, Lorenzo. 2021. "The EU's Permanent Structured Cooperation, NATO, and the US: beyond a zero-sum game". https://www.coleurope.eu/sites/default/files/research-paper/giuglietti_cepob_5.pdf.

Hancock, Dawson, Bob Algozzine, and Jae Hoon Lim. 2021. "Doing Case Study Research". 4th Edition. Teachers College Press. 2021.

Ilinca, Dragoș. 2022. "The Role of Permanent Structured Cooperation in the Development of Defence Capabilities". *Strategic Impact*, no. 2: 7-20. https://revista.unap.ro/index.php/Impact_en/article/view/1590/1540.

Martill, Benjamin, and Carmen Gebhard. 2023. "Combined differentiation in European defense: tailoring Permanent Structured Cooperation (PESCO) to strategic and political complexity". *Contemporary Security Policy*, vol. 44, no. 1: 97-124. 2023. https://www.tandfonline.com/doi/epdf/10.1080/13523260.2022.2155360?needAccess=true.

Michaels, Eva and Monika Sus. 2024. "(Not) Coming of age? Unpacking the European Union's quest for strategic autonomy in security and defence". *European Security*, vol. 33, no. 3: 383-405. https://www.tandfonline.com/doi/epdf/10.1080/09662839.2024.2376603?needAccess=true.

Permanent Structured Cooperation. 2025a. "PESCO Participating Member States". https://www.pesco.europa.eu/about/.

___. 2025b. "Projects". https://www.pesco.europa.eu/.

___. 2025c. "CBRN Defence Training Range (CBRNDTR)". https://www.pesco.europa.eu/project/cbrn-defence-training-range-cbrndtr/.

___. 2025d. "European Union Network of Diving Centres (EUNDC)". https://www.pesco.europa.eu/project/european-union-network-of-diving-centres-eundc/.


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


Institutional Evaluation Programme
Performance in Research, Performance in Teaching – Quality, Diversity and Innovation in Romanian Universities Project

"CAROL I - NATIONAL DEFENCE UNIVERSITY"
BUCHAREST-ROMANIA

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: 06.10.2025
The publication consists of 356 pages.

639/06.10.2025

C.212/2025