BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

No. 4/ 2024

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, 2024

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. 4/2024

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Key Milestones in Urban Operations

LTC Claudiu-Valer NISTORESCU, Ph.D.*

*Command and Staff Faculty / "Carol I" National Defense University, Bucharest, Romania
e-mail: nistorescu_claudiu@yahoo.com

Abstract

Both the Russian-Ukrainian war and the conflict in the Gaza Strip underline the importance of the cities and urban terrain in combat operations. The battles for Kiev, Mariupol, Bakhmut, Gaza, and Rafah demonstrate the scale, intensity, and ferocity of the combatants' actions, as well as the sensitivity of the operational process in the context of a transparent and highly contested operational environment. The new demands of today's operational environment require adjustments to the planning process preparing and execution of the military operations. The urban environment, by its specificity, generates a series of implications for combat operations, which become essential benchmarks of the operational process.

In this context, the objective of this paper is to identify and describe the milestones of the operational process related to urban operations. While the results of the research offer empirical solutions, their value is enhanced by the theoretical contribution they make to tactical-level commanders in terms of the approach to this type of operation.

Keywords:

combat operations; urban environment; urban triad; combined-arms warfare.

Article info

Received: 18 October 2024; Revised: 25 November 2024; Accepted: 4 December 2024; Available online: 17 January 2025

Citation: Nistorescu, C.V. 2024. "Key Milestones in Urban Operations".
Bulletin of "Carol I" National Defence University, 13(4): 7-21. https://doi.org/10.53477/2284-9378-24-45

Recent estimates and expert studies indicate that the global population will reach 9.8 billion by 2050, an increase of 2.1 billion from the current figure. The growth will be gradual but disparate on a global scale, with Asia, South America, and Africa exhibiting particularly rapid expansion. Concurrently, an increasing proportion of the population will opt to reside in urban areas, resulting in the expansion of urban settlements and the stimulation of economic growth. However, this phenomenon will exert pressure on governmental institutions, particularly in developing countries (UK Ministry of Defence 2024, 13). Furthermore, by the middle of the century, it is projected that approximately 60.5% of the global population will reside in urban areas, representing a notable increase from the current estimate of 48.3% of the total population employed in urban settings (UK Ministry of Defence 2024, 126).

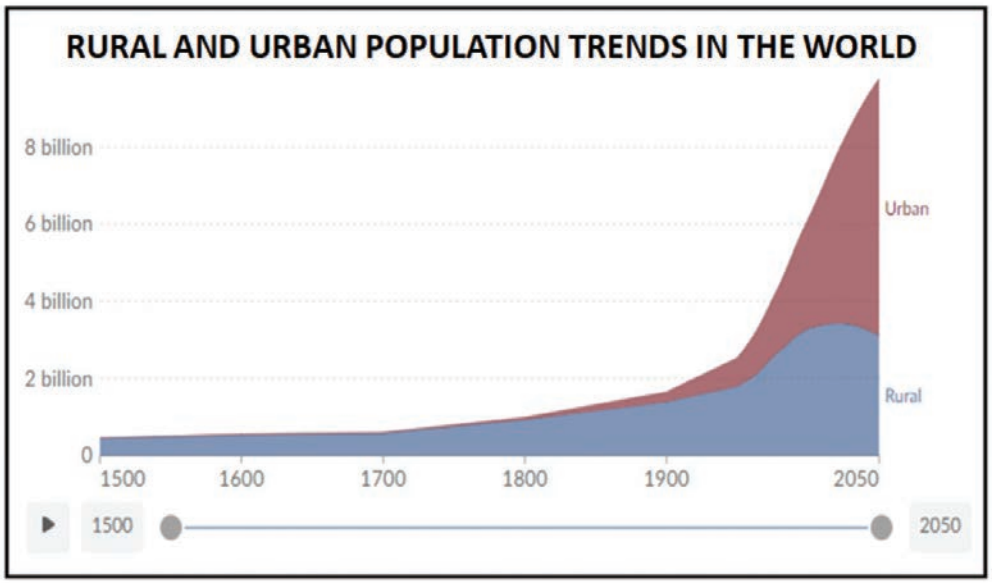


Figure 1 Comparative rural and urban population trends in the world (period 1500-2050)
Source: Hannah Ritchie, Max Roser, *Urbanization*, https://ourworldindata.org/urbanization, accessed on 12.11.2024.

In this context, studies conducted at the allied level, based on an analysis of demographic trends, the evolution of the geostrategic and security environment, the development of high technologies and their influence on society, indicate an increase in the frequency of armed conflicts in urban environments (NATO 2018). In his analysis, Canadian security specialist Robert Muggah posits that urban areas will become the new frontier of war in the context of global conflict (Muggah 2015) and Lawrence Freedman posits that megacities will become the epicenters of human activity on the planet, and thus the site of the majority of conflicts necessitating military intervention (Freedman 2019, 349).

The heightened sensitivity of conflicts in urban environments is a consequence of the distinctive attributes inherent to such settings. The physical agglomeration of urban environments, both horizontally and vertically, coupled with the presence of underground networks, critical infrastructure elements, a congested electromagnetic

environment, extensive media facilities, and the human factor, collectively serve to render military operations in such particularly challenging settings. The experience of past conflicts demonstrates that the destructive capacity of urban environments can be a significant factor in military operations. The adage "cities destroy armies and armies destroy cities" is illustrative of this phenomenon (Chychota 2019, 295). The hypothesis is validated by contemporary armed conflicts, witnessing the battles of Mariupol, Bakhmut, Avdiivka, Gaza, and Khan Yunis.

In light of the heightened probability of armed conflicts in urban settings, a comprehensive evaluation of the operational procedures for such confrontations is imperative. The topic of urban warfare has attracted considerable interest from military theorists and leaders, with a substantial body of literature examining the implications of cities for the design of strategic operations (Department of the Army Headquarters, TRADOC Pamphlet 525-92-1 2020), the need to achieve effects at the joint level of operations to fulfill the conditions necessary to achieve the desired end state (US Joint Chiefs of Staff, JP 3-06 2013) and the difficulty of decentralized tactical operations down to the lowest level (NATO, ATP-3.2.1.2 2022).

The objective of the analysis is twofold: firstly, to describe the principal milestones that have shaped our understanding of the urban environment; and secondly, to identify the factors that have led to a need for change in the specific operations of urban armed combat. Finally, from the standpoint of these findings, the principal objective of the research is to ascertain the doctrinal and operational implications that have emerged as a consequence of the new demands of the contemporary operational environment, both in terms of action and organization.
In order to direct the research effort, we sought to address the following questions:

- What are the fundamentals of combat operations conducted in the context of urban environments?
- What are the factors that make it necessary to reconsider armed combat in the urban environment?
- What are the implications for urban operations in the context of the new requirements of the operating environment?

The interrogation of open sources about the conduct of combat operations in the conflicts in Ukraine and the Gaza Strip has yielded empirical results. It is imperative to enhance these findings and corroborate them through the utilization of war gaming and military exercises. Moreover, it is important to consider the possibility that some data and information may have been altered to some extent, either due to operational security requirements or the intention to mislead and influence the warring parties.

The understanding of the urban environment and the fundamentals of urban operations

The complexity of the urban environment, and thus the difficulty of related military operations, arises from the existence of a multitude of multidimensional systems and

subsystems, which are both interconnected and interdependent. These systems can be classified as either physical or non-physical, including the physical system, the population, and the information system. (Department of the Army Headquarters ATP 3-06, MCTP 12-10B 2017, 1-3). Collectively, these elements constitute what military analysts refer to as the *urban triad*.

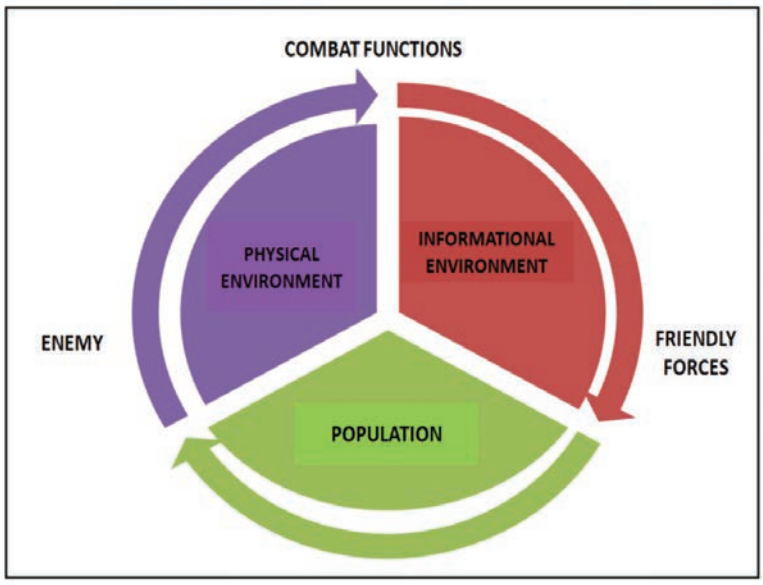


Figure 2 Urban triad
Source: Department of the Army Headquarters ATP 3-06, MCTP 12-10B 2017, 1-3.

The physical system of the urban environment is constituted by the land features. The urban terrain comprises two principal components: a natural component, comprising landform details, and an artificial component, comprising infrastructure and human-made constructions. In addition, the urban terrain includes the space in the vicinity of human settlements. The physical system is characterized by the imprint of the main attributes of the natural component in terms of the spatial configuration of the city. Concurrently, the anthropogenic element is shaped by the extent of economic advancement, the prevailing cultural norms, and the social stratification of the population.

The population constitutes the core of the urban system and plays a pivotal role in influencing the conduct of military operations. The city is divided into distinct socio-economic zones, comprising affluent residential areas, middle-class residential areas, and poor suburban areas. The type and layout of buildings, existing facilities, and the varying population densities in these areas may influence the approach to combat operations in urban areas. It is also incumbent upon military planners to take into account the economic factor, as well as ethnic, cultural, and religious diversity. Inevitably, the total evacuation of the civilian population from urban areas during periods of conflict will not be feasible (Arnold and Fiore 2019). The battles in Mosul, Ramadi, and also in Mariupol, and Gaza serve to corroborate this assertion.
The information system encompasses all communication systems and networks

pertaining to the urban center. The system is distinguished by a high degree of fluidity, with interconnections to the local infrastructure and a capacity to be influenced by human interaction (NATO Standard, AJP-3.2 2022, A-3). A further crucial aspect of this system is the continual alteration of its constituent elements and procedures, which exerts an impact on the operational context and on how commanders and their staffs interact with it. The high degree of permeability of this system provides opportunities for all actors. In light of the sensitivity and unpredictability of actions in the cyber domain and the electromagnetic spectrum, coupled with the difficulty of preventing and countering them, a complex asymmetric threat environment emerges. The asymmetry inherent to these environments arises from the potential for hostile actors to undertake actions without adherence to international law (Pamment, et al. 2019, 61). Although the exploitation of information systems can confer significant advantages upon friendly forces, enabling the influence of the population and the creation of an environment favorable to the execution of the operation, it also provides adversaries with a relatively straightforward means of influencing military operations.

It is imperative that military operations in urban environments consider these systems, as their manifestation influences the operational process irrespective of the campaign rationale or the nature of the operation. In light of the significant influence that the local population can exert on military operations, military planners must consider the necessity of conducting operations that encompass the full spectrum of their potential manifestations, including combat operations, security, and peace support operations. In addition, the tactical actions that may be employed within these types of operations include offensive and defensive actions, counter-insurgency operations, counter-terrorism, humanitarian assistance, the evacuation of non-combatants, support to local authorities, and so forth. Nevertheless, in addition to the examination of these systems, a PMESII analysis of the urban environment is essential for a comprehensive evaluation of the urban environment and to gain a coherent understanding of a potential setting for military operations. Furthermore, in the context of tactical operations, it is imperative that intelligence preparation of the battlefield exercise due consideration of the civilian component, which has the potential to exert a decisive and irreversible influence on the conduct of operations, thereby either enhancing or undermining the prospects of success.

Key factors to reconsider urban operations

In recent decades, Western militaries have concentrated their resources on responding to the challenges posed by large-scale, low-intensity conflicts in the Middle East and North Africa. The demands of counter-insurgency operations have shaped a number of defining features in military doctrine, force configuration, training, and the equipping of combat technology and weapons systems. Furthermore, the prioritization of the civilian population in military operations

has necessitated the development of a distinctive approach to warfare, with a considerable influence on the design of these operations. Potential adversaries of the Western armies have frequently been able to nullify their quantitative and qualitative superiority by employing asymmetric and unconventional methods and capabilities. Consequently, many conventional capabilities were overlooked, as was conventional warfare training (Scrogin 2019, 19-20). The necessity to preserve the security of the population while simultaneously defeating an ill-defined adversary led to the adoption of a minimum casualty-oriented approach among the own forces. In light of these considerations, and also taking into account the increased likelihood of the materialization of conventional armed conflicts, it is evident that *a transition from counter-insurgency operations to specific armed combat operations is required.* This transition must be made in both a mental and physical sense. The rethinking of military doctrines, reconfiguration of tactical formations, and reconstitution or revitalization of conventional capabilities are contingent upon the mental acceptance of this necessity by political and military leaders.

The necessity to integrate operations at the multi-domain level is also a factor in the imperative to rethink military operations in the urban environment. The convergence of effects from all domains of operations, including actions in the electromagnetic spectrum, cyber, and information, has prompted military specialists to redefine the defining benchmarks of military operations in order to maintain relative military superiority. The North Atlantic Alliance's foundational doctrine defines multi-domain operations as the orchestration of all military and non-military actions across all domains of operation, with the objective of ensuring the timely and effective delivery of effects (NATO Standard, AJP-1 2022, 3). The complexity of combat operations in an urban environment and their extension beyond the dimensions of classic areas requires the concerted use of specific *"capabilities in all domains of the battlespace, which are aimed at achieving success in the most effective way."* (Vereș 2024).

The advent of new technologies and weapon systems has had a significant impact on the evolution of tactics, techniques, and operational procedures. Furthermore, the enhanced lethality of modern combat is a direct consequence of the advent of new technologies and weapon systems. The extended range, enhanced accuracy, and diversification of multispectral sensors have facilitated the advancement of these technologies.
A further factor that necessitates a reassessment of particular urban combat operations is the enhanced visibility of the battlefield. As the battlefield becomes more technologized, *"it has become increasingly difficult to conceal military forces and actions nowadays"* (Toroi 2024), forcing military commanders to look for new innovative and creative ways to hide their intentions and forces. Finally, the algorithm of potential enemy combat influences the doctrinal and operational adaptation of Western forces. The operational behavior of the Russian forces in Ukraine allows for the identification of an algorithm that places significant emphasis on the central role of artillery, the capacity to accept a considerable number of casualties among

one's own forces, and tolerance for casualties and collateral damage. It would appear that the Russian model is based on an approach centered on the historical balance of forces, which does not satisfy the requirements of the dispersion principle. Furthermore, it draws attention to the ineffectiveness of modeling operations and the overuse of imprecise strike vectors. The disproportionate destruction carried out by the Russian army to achieve the tactical objectives of the siege of Mariupol and the battles for Bakhmut and Avdiivka is evidenced by the sieges themselves and the battles that preceded them (Butler 2023).

Implications arising from factors requiring reconsideration of urban operations

The factors that generate implications for operations in the urban environment are reflected in the operational process and have a direct impact on the combat functions, the organization, and the composition of tactical formations, tactics, and operating procedures.

Combat functions

In conceptual terms, combat functions represent "the principal tools at the disposal of the commander, which he integrates and coordinates within operations in order to synchronize effects in terms of time, space and purpose." (Statul Major al Forţelor Terestre 2017, III-13). The integration of these elements into the fighting power of tactical formations, in accordance with the requirements of the operational environment and enemy actions, is the foundation upon which the combat effectiveness of those formations is built. The urban environment is distinctive in terms of the manner in which these functions are integrated, and thus it is essential to conduct an analysis in order to ascertain the necessity for reconsideration of urban operations and to identify potential solutions for their adaptation. In light of the aforementioned considerations, the analysis encompasses a range of operational aspects, including command and control, intelligence support, maneuver, fires, force protection, and sustainment.

• *Command and control*

In an urban environment, command and control is particularly susceptible to disruption due to the necessity for decentralized operations. This, in turn, gives rise to the need for force disaggregation and the implementation of additional measures to ensure the synchronization of actions and the coordination of forces. Agglomeration of the electromagnetic environment, and the vertical development of the urban terrain, restrict communications. Obstruction of observation fields requires drastic control measures to avoid fratricide or collateral casualties. It is therefore essential to ensure the continuous updating of the forces' position in order to guarantee the success of the operation and the timely execution of the required support. The most accurate means of monitoring position is through the use of

Global Positioning Systems (GPS). The deployment of satellite imagery or drones for the surveillance of forces engaged in densely populated areas also serves to enhance their control capability. Nevertheless, the efficacy of these capabilities may be constrained in densely populated urban areas and in the face of multifaceted challenges to one's own forces. In such contexts, where ambiguity and uncertainty prevail, the autonomy of decision-making and initiative on the part of commanders is indispensable for the effective conduct of the operational process.

• *Intelligence*

The integration of intelligence as a function of combat presents particularities generated by the specificity of the confrontation environment, and the difficulty of obtaining timely and accurate information is evident. The perishability of information is high, due to the reduced possibilities of maintaining positive identification/PID. As a result, the find-detect-identify-surveil cycle has to be repeated more often than under other conditions and requires significantly more reconnaissance capabilities and elements. In most cases, the human factor is decisive, but various sensors produced by new technologies can complement human resources. Thus, UAS, IMINT, SIGINT, but also MASINT capabilities become valuable tools in this highly constrained environment. During conventional operations, particularly offensive operations, commanders should employ HUMINT capabilities to obtain information from resident civilians, refugees, and displaced persons, and to interrogate detainees and prisoners of war (Department of the Army, FM 2-0 2023, 1-18).

• *Maneuver*

The maneuverability of conventional forces is severely restricted in an urban environment, and the actions of mounted forces are channeled along the streets. The fragmented nature of the terrain requires a compartmentalized and methodical approach to combat operations, creating the need to divide the city into rectangular areas of operation, clearly delineated by streets and corresponding to the capabilities of the unit to which it is assigned. Buildings, canals, and other infrastructure create obstacles for the attacker and favor the defender. In most cases, the capturing and securing of an objective implies seizing and securing each building, complex of buildings, and that is why the maneuver of forces in an urban environment has a reduced speed. The experience of the Israeli forces in the Gaza Strip shows that it is not advisable to assign non-contiguous areas of operation to the forces engaged in the main lines of the offensive (Watling and Reynolds 2024, 1). The use of armored forces in urban environments must be based on a careful assessment of the threat, with the infantry-tank binomial most often being the appropriate solution for urban maneuvers. The success of maneuver operations depends to a large extent on the provision of cover forces to neutralize enemy anti-tank elements, ambushes and snipers, and light infantry elements to provide close protection for armored vehicles. Commanders must therefore strive to achieve an optimum balance between mounted and dismounted forces. The maneuver of armored forces can be facilitated by shaping operations carried out by forward detachments or tactical airdrops.

However, these tactical capabilities have relatively low combat power and are limited in their ability to sustain operations. Finally, the success of maneuver forces is contingent upon the efficacy of fire support and the capacity to guarantee force mobility. Based on the insights gained, it can be posited that artillery strikes may yield a favorable outcome in the context of the immediate tactical situation. However, such strikes inevitably result in destruction, which subsequently constrains maneuver possibilities. Consequently, it is imperative to integrate engineer capabilities with maneuver elements to ensure the clearance and establishment of mobility corridors (Department of the Army Headquarters, TRADOC Pamphlet 525-92-1 2020, 19).

• *Fire support*

Fire support is more difficult to achieve in urban environments, on the one hand, because of the fragmentation of the terrain and the difficulty in spotting and identifying targets, and on the other because of the risk of collateral damage and casualties. Although the recent conflicts in Ukraine and the Gaza Strip highlight the propensity of the forces to use their fire support capabilities, they retain only a shaping role, with maneuver forces' action being necessary to defeat the enemy (Mirea 2024). Furthermore, the probability of fratricide is elevated when observation and firing sectors are obstructed. In this regard, the implementation of effective fire support control measures and the utilization of collateral damage estimation (CDE) are of paramount importance. It is therefore essential that fire support capabilities be tailored to the intended effects. While the use of smart munitions may be advantageous, it is imperative to consider the potential risk of jamming. The most appropriate anti-tank weaponry is that which is portable and guided, such as anti-tank missile systems. The aforementioned capabilities, through their fire-and-forget, top-attack, or flying top-attack functions, prove to be highly advantageous in urban combat. The battle for Kyiv in the initial phase of the conflict in Ukraine serves as an illustrative example in this regard (Johnson 2022).

• *Protection*

In light of the reduced operational tempo and constrained maneuverability, there is a compelling need for multidimensional protection in the urban environment for both mounted and dismounted forces. It is only through the coordination of maneuver and mutual support actions, both at the level of the aforementioned capabilities and between adjacent tactical formations, that the specific vulnerability of those elements can be reduced (NATO, ATP-3.2.1.2 2022). Furthermore, there is a significant requirement to provide protection for military personnel against a range of potential threats, including ambushes, sniper attacks, unmanned aerial vehicles (UAVs), and improvised explosive devices (IEDs). In this context, the provision of cover and security elements acquires considerable importance.

• *Sustainment*

The urban environment exerts considerable pressure on the logistical system, particularly in the context of combat operations. Ammunition consumption is high,

supply routes can be easily intercepted by the enemy, and medical evacuation is often by land. However, the urban environment provides a number of facilities to combatants, even if these are only temporary and should not be incorporated into the operational equation. These include sources of electricity, food and water, civilian medical facilities, accommodation and shelter, and so on.

Force organization and composition

The initial phase of the Russian Federation's invasion of Ukraine revealed the shortcomings and ineffectiveness of the battalion-level tactical groups (BTGs) deployed in offensive operations, including those conducted in urban centers (Jones 2022). Despite their independent operational capabilities, including in urban environments, these units could not be integrated as a unified force into large-scale offensive operations. Moreover, they were unable to benefit from the intended effects of the shaping operations that were to be conducted by the upper echelons in their support (Kofman and Lee 2022).

Consequently, the Russian Federation has abandoned the use of battle groups in favor of a return to the traditional configuration of tactical structures, comprising regimental and divisional units. In operations conducted in urban environments, these have been superseded by the introduction of assault detachments, which offer enhanced flexibility and adaptation to the specific conditions of such environments (Nistorescu 2024).

There is no definitive formula for the organization of tactical structures for urban combat. However, in the context of combat operations against an enemy with conventional and relatively equal capabilities, it is necessary to achieve a mix of forces, including heavy armor (tanks or infantry fighting vehicles), medium infantry (armored personnel carriers), and light infantry mounted on light armor and dismounted infantry. Furthermore, additional elements are incorporated, including artillery, air defense, combat engineers, and armored reconnaissance, as well as airborne capabilities. In the context of the military operations conducted in the Gaza Strip, the Israeli army has predominantly deployed brigade-level structures, comprising one heavy armored (tank) battalion, one mechanized battalion, one light infantry battalion, one engineer battalion, one artillery battalion, one special operations forces detachment and combat support elements decentralized down to the subunit level (Watling and Reynolds 2024).

Tactics techniques and procedures (TTPs)

The maintenance of relative superiority over the enemy is a fundamental aspect of TTPs, particularly in the context of multiple simultaneous clashes and tactical engagements. Furthermore, the decentralization of operations entails a decentralization of forces and capabilities, notably including support forces and capabilities. The success of combat operations hinges on a multitude of factors, including a comprehensive understanding of the operational environment and the

interrelationship between one's forces, the enemy, and the civilian population. It is imperative to recognize that one's forces are subject to constant monitoring and to seize and exploit advantageous positions, whether physical, informational, or derived from the perspective of the civilian population.

The initial contact with the enemy should be made with the smallest possible element, and challenges, options, and criteria for transition must be anticipated and identified. Gains must be consolidated and morale maintained. In the context of urban operations, the use of surprise, the rapid pace of action, and the ability to respond swiftly and effectively are crucial elements of successful tactics. Raids have the potential to inflict significant damage on enemy combatants, affecting both their physical and psychological capabilities. The contribution of airborne or air assault forces to the success of an operation must be weighed against their vulnerability, given the inherent limitations in space and time that constrain their combat possibilities. The failure of the Russian airborne operation to seize the Hostomel airport near the Ukrainian capital, Kyiv, is a matter of historical record that serves to exemplify this fact Kiev (Collins, Kofman and Spencer 2023).

The necessity for a three-dimensional approach to the terrain remains a significant concern, as evidenced by the experience of the conflict in the Gaza Strip. This highlights the importance of blocking off underground canals and tunnels, controlling basements and ground floors of buildings, as well as intermediate floors. However, there has been a notable decline in the tendency to occupy the top level of buildings or their roofs. This significantly reduces freedom of maneuver, with opportunities for observation from above being supplemented by drones (Watling and Reynolds 2024, 6).

In the context of the high-intensity conflict in Ukraine, tanks were seldom employed as the primary assault element in urban combat. However, they were assigned to assault detachments and performed fire support for infantry, as well as penetrating non-explosive barrages or creating access routes through rubble on communication routes (Watling and Reynolds 2023, 16).

Conclusions

The analysis provides an answer to the research questions and also highlights the necessity for the adaptation of the forces and the operations performed by them. Furthermore, it highlights the necessity of meticulous and continuous examination of the evolution of the operating environment as a prerequisite for fostering innovation and adaptation. The experience of recent military conflicts illustrates the fact that the conduct of military operations in urban environments necessitates a constant process of transformation and continuous adaptation, both in terms of doctrine and operational procedures. These transformations encompass a reconsideration

of conceptual approaches, an adjustment of tactics, techniques, and procedures, an organizational and compositional recalibration of tactical formations, the provision of new weapon systems and military equipment, the implementation of force training, and leader development. The adaptation of operations translates into a series of measures aimed at creating and employing combined arms formations tailored to the specific characteristics of the operating environment. The goal is to seize control of key terrain and critical infrastructure within the city, thereby leveraging the urban system effectively. The management of the local population, the containment of threats, the minimization of collateral damage and casualties, and the maintenance of the integrity of urban systems are also key considerations. Furthermore, the creation of a collaborative environment conducive to the cessation of hostilities and the transition to stability operations is essential.

It can be observed that combat operations retain their primacy in terms of difficulty and intensity, as well as the scale of casualties and disproportionate destruction. Despite the high costs involved, the materialization of urban combat remains a certainty, largely due to the tendency of the weaker side to exploit the advantages of the urban environment. It can be seen that defensive operations are advantaged, with research results indicating that the initiative is lost by the attacker once the forces enter the city. The pace of the offensive is slowed, with the necessity for the attacker to repeat the find-fix-strike cycle becoming increasingly prevalent. It is not feasible to completely isolate large cities, and the urban infrastructure allows defending forces to maintain their position for extended periods, particularly in industrial areas. It is similarly unlikely that the entire civilian population will be evacuated. Consequently, it falls upon the forces to address the challenges posed by the presence of civilians in the operational area. The most significant challenge lies in the ability to transition from combat operations to stability operations and vice versa. To achieve this, it is essential to ensure that tactical land forces receive comprehensive training and are adequately equipped. However, the most crucial aspect is to ensure that they are mentally prepared to make this transition effectively. The inherent risks associated with this period of change can be attributed to two key factors: the difficulty in accurately assessing the level of threat and the sensitivity of the transfer of authority between armed forces and government institutions.

In light of the technological aspect, it can be posited that the evolution of military operations in urban settings will be contingent upon the advancement of cutting-edge, nascent, and transformative technologies. It can be reasonably predicted that these will result in the advent and evolution of novel weapon systems that will have a considerable impact on tactics, techniques, and combat procedures. It is anticipated that the general trends in the evolution of weapon development will persist, with a continued focus on extending range and improving accuracy, coupled with enhanced target identification algorithms and the differentiation of civilians from hostile elements. The frequency of use of unmanned capabilities, including autonomous ones, represents another significant factor influencing the evolution of

urban operations. While these capabilities may initially be employed on secondary routes, for cover, reconnaissance, and surveillance missions, or as part of misleading operations, their broader integration into urban operations is likely to become increasingly prevalent. Nevertheless, despite the unprecedented technological advancement of the battlefield and its enhanced transparency, the adaptability of adversaries and the intricacy of the urban environment provide the foundation for leveraging its advantages.

It bears reiterating that the human element will continue to be of paramount importance in the context of military operations conducted in urban environments. Due to their distinctive capacity to engage with the civilian population, as well as with government and local authorities, ground forces will be the primary instrument in future conflicts. Their attributes afford them the capability to neutralize threats, resolve existing differences, and achieve the desired end state.

References

Arnold, Thomas D., and Nicolas Fiore. 2019. "Five Operational Lessons from the Battle for Mosul." *Military Review.* https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-19/Arnold-Fiore-Lessons-Mosul.pdf.

Butler, Marcus. 2023. "Russia's Response to the Challenges of Urban Warfare in the Russo-Ukrainian War." *Towson University Journal of International Affairs.* https://wp.towson.edu/iajournal/2023/01/13/russias-response-to-the-challenges-of-urban-warfare-in-the-russo-ukrainian-war/.

Chychota, Michael T. 2019. *Large-Scale Combat Operations in Urban Terrain.* Editor US Army Command and General Staff College Press Book. Vol. Large-Scale Combat Operations – The Division Fight. Army University Press.

Collins, Liam, Michael Kofman, and John Spencer. 2023. "The Battle of Hostomel Airport: A Key Moment in Russia's Defeat in Kyiv." *War on the rocks.* https://warontherocks.com/2023/08/the-battle-of-hostomel-airport-a-key-moment-in-russias-defeat-in-kyiv/.

Department of the Army Headquarters ATP 3-06, MCTP 12-10B. 2017. *Urban Operations.* United States Marine Corps.

Department of the Army Headquarters, TRADOC Pamphlet 525-92-1. 2020. *The Changing Character of Warfare: The Urban Operational Environment.* Fort Eustis, Virginia: U.S. Army, Training and Doctrine Command. https://adminpubs.tradoc.army.mil/pamphlets/TP525-92-1.pdf.

Department of the Army, FM 2-0. 2023. *Intelligence.* Headquarters, Department of the Army.

Freedman, Lawrence. 2019. *Viitorul războiului.* Bucureşti: Editura Litera.

Johnson, David. 2022. "The Tank Is Dead: Long Live the Javelin, the Switchblade, the… ?" *War on the rocks.* https://warontherocks.com/2022/04/the-tank-is-dead-long-live-the-javelin-the-switchblade-the/.

Jones, Seth G. 2022. "Russia's Ill-Fated Invasion of Ukraine: Lessons in Modern Warfare." *Center for strategic and international studies.* Edited by Center for Strategic and International Studies. https://www.csis.org/analysis/russias-ill-fated-invasion-ukraine-lessons-modern-warfare.

Kofman, M., and R. Lee. 2022. "Not Built For Purpose: The Russian Military's Ill-Fated Force Design." *War in the rocks.* Edited by War on the Rocks. https://warontherocks.com/2022/06/not-built-for-purpose-the-russian-militarys-ill-fated-force-design/.

Mirea, Adrian. 2024. „Pregătirea de foc a ofensivei – necesitatea actualizării algoritmului de planificare." *Buletinul Universității Naționale de Apărare „Carol I"* 13 (3): 126-136.

Muggah, Robert. 2015. "Fixing Fragile Cities." https://www.foreignaffairs.com/articles/africa/2015-01-15/fixing-fragile-cities.

NATO. 2018. *Framework for Future Alliance Operations.* Bruxel: NATO Standardisation Office.

NATO Standard, AJP-1. 2022. *Allied Joint Doctrine.* Vols. Edition F, Version 1. Bruxel: NATO Standardization Office (NSO).

NATO Standard, AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations.* Vol. Edition B Version 1. Bruxel: NATO Standardization Office (NSO).

NATO, ATP-3.2.1.2. 2022. *Conduct of Land Tactical Operations in Urban Environments.* Vols. Edition A, Version 1. Bruxel: NATO Standardization Office (NSO).

Nistorescu, Claudiu-Valer. 2024. *Forțele Terestre ale Federației Ruse.* București: Centrul tehnic-editorial al armatei.

Pamment, James, Vladimir Sazonov, Francesca Granelli, Sean Aday, Māris Andžāns, Una Bērziņa-Čerenkova, John-Paul Gravelines, *et al.* 2019. "Hybrid Threats: 2007 cyber attacks on Estonia." NATO Strategic Communication Centre of Excellence. 52-69. https://stratcomcoe.org/publications/hybrid-threats-2007-cyber-attacks-on-estonia/86.

Scrogin, James D. 2019. *Large-Scale Combat Operations: Relearning an Old Concept.* Editor US Army Command and General Staff College Press Book. Vol. Large-Scale Combat Operations – The Division Fight. Army University Press.

Statul Major al Forțelor Terestre, F.T.-1. 2017. *Doctrina operațiilor forțelor terestre.* București: Statul Major al Forțelor Terestre.

Toroi, George. 2024. „Reziliența – multiplicator al efectelor în pregătirea contracarării inducerii în eroare." *Buletinul Universității Naționale de Apărare "Carol I"* 13 (3): 111-125.

UK Ministry of Defence. 2024. *Global Strategic Trends.* Seventh Edition. https://assets.publishing.service.gov.uk/media/673602412469c5b71dbc7b6f/Global_Strategic_Trends_Out_to_2055.pdf.

US Joint Chiefs of Staff, JP 3-06. 2013. *Joint Urban Operations.* US Joint Chiefs of Staff. https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_06.pdf.

Vereș, Petru-Marian. 2024. „Integrarea capabilităților multidomeniu în operațiile unităților interarme din forțele terestre." *Buletinul Universității Naționale de Apărare "Carol I"* 13 (1): 44-59.

Watling, J., and N. Reynolds. 2023. *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine.* Londra: Royal United Services Institute for Defence and Security Studies/RUSI.

___. 2024. *Tactical Lessons from Israel Defense Forces Operations in Gaza, 2023.* Londra: Royal United Services Institute for Defence and Security Studies.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Incorporating "Security" in Sustainable Development Goals (SDG): Insights from Food Security and Climate Change

Ayfer Genç YILMAZ*
Gülşah SEDEFOĞLU**

*Istanbul Ticaret University, Department of Political Science and International Relations
e-mail: agenc@ticaret.edu.tr.
**Istanbul Ticaret University, Department of Statistics
e-mail: gsedefoglu@ticaret.edu.tr.

Abstract

After drawing a theoretical framework based on a reciprocal approach for understanding the relationship between security and development, the paper suggests a causal diagram in which all Sustainable Development Goals (SDGs) occur as an interdependent whole and security is embedded as "Goal 0" to symbolise the link from security to development or vice versa. The diagram unveils the interaction between development and human and state dimensions of security, arguing that the definition of security cannot be limited to nonviolence or peace. Instead, the diagram emphasises that security, akin to development, is a multidimensional concept. The paper thus brings a comprehensive approach to security, emphasising the interdependence between human and state security, and highlighting how both perspectives contribute to development. By incorporating security in SDGs and making it more visible, the paper aims to bring a solution-oriented perspective to the policy-making process. Finally, the paper discusses the nexus between development and security through the analysis of two cases within SDGs: climate change and food security. The paper concludes that incorporating security in SDGs can provide a basis for implementing effective policies in the transition from sustainable development to sustainable security and successfully putting forward the 2030 agenda for the SDGs.

Keywords:
security; development; sustainable development goals; security-development nexus.

Article info
Received: 6 October 2024; Revised: 4 November 2024; Accepted: 26 November 2024; Available online: 17 January 2025

Citation: Yilmaz, A.G., and G. Sedefoğlu. 2024. "Incorporating "Security" in Sustainable Development Goals (SDG): Insights from Food Security and Climate Change". *Bulletin of "Carol I" National Defence University*, 13(4): 22-36. https://doi.org/10.53477/2284-9378-24-46

The end of the Cold War sparked a significant rethinking of security. Constructivist approaches led the way, shifting focus from the state and military towards a wider range of actors and threats (Buzan, Waever and De Wilde 1998, 6). A key moment was the 1994 introduction of human security by the United Nations Development Program (UNDP). This concept highlighted the interconnected nature of security and development, prompting new avenues of analysis. Despite ongoing debate about the complexities and implications of this relationship across different levels – international, national, and individual – the idea that security and development are mutually dependent has gained traction in both fields.

This paper examines the complex relationship between development and security, questioning whether the Sustainable Development Goals (SDGs) should explicitly include "security" as a standalone goal. While the SDGs, adopted in 2015 as successors to the Millennium Development Goals (MDGs), address a broad spectrum of issues, they lack a dedicated security focus. This omission is notable given that the interdependence of security and development has been widely acknowledged. Even the MDGs, established in 2000, included direct references to global peace and security (Stern and Ojendal 2010, 6). Instead of a distinct security goal, the SDGs incorporate elements of security within Goal 16, which emphasizes peace, justice, and strong institutions (The UN General Assembly 2015). This approach, however, arguably fails to give the concept of security the prominence it deserves.

Many scholars explore the connection between development and security from a critical perspective (Duffield 2017; Beall, Goodfellow and Putzel 2006; Klingebiel 2006) and in different historical geopolitical contexts (Hettne 2010). Duffield (2017) explores how the war on terrorism has deepened the interconnection between development and security. He takes human security as "a technology that empowers international institutions and actors to individuate, group, and act upon Southern populations." In this regard, the balance between development and security transformed to act in favour of security and at the expense of development (Beall, Goodfellow and Putzel 2006), thus prioritizing homeland livelihood systems (Duffield 2017, 13). Similarly, Klingebiel (2006) explores the potential dangers and risks of the securitization of development policy. From a different perspective, Stewart (2013) concludes that the insecurity will impact development through poverty and the lack of development, along with the horizontal inequalities, largely causes conflict. Khagram et al. (2003) underline the linkage between sustainable development and sustainable security. Keukeleire and Raube (2013) examine the EU development policies in terms of its security implications. Cilliers (2006) emphasizes the interdependence of development and security in post-conflict interventions. Finally, De Simone and Iocchi (2022) question whether the security-development nexus came to an end.

This paper makes three key contributions to existing literature. First, it proposes that the relationship between development and security is reciprocal and interconnected.

Achieving security and development go simultaneously, reinforcing each other. Development flourishes in secure environments, while security relies on a certain level of economic development. Despite the UN's frequent acknowledgement of the humanitarian-development-peace nexus (Guterres 2016, 2017, 2018), practical implementation remains a challenge. This paper seeks to address this gap by advocating for a standalone "security" goal within the SDGs. It proposes designating security as "SDG Zero" to emphasize its foundational role, underscoring that all other goals are contingent on ensuring security for both states and individuals.

Second, the paper champions a comprehensive approach to security, recognizing the complementary nature of human and state security. It argues that both dimensions are linked to development, and therefore, their inclusion is crucial for a complete understanding of the SDGs.

Finally, the paper examines the intricate connections between development, security, and the interplay of human and state security through the lenses of food security and climate change – two prominent themes within the SDGs. By highlighting the interconnectedness of various SDGs, it underscores the need for a causal framework to analyze these complex relationships.

This paper relies on an interpretive research design and focuses on understanding social meanings embedded within international politics. Interpretive research often relies upon case studies that focus on the use of discourses in a given context (Lamont 2015, 43). We want to understand how the SDGs should be redesigned to include state and human security by investigating the case of food security and climate change.

First, we explore the ongoing debate surrounding the relationship between development and security, emphasizing the mutually interconnected nature of this connection. We argue that development and security are mutually reinforcing, each requiring the other to thrive. Next, we propose a restructuring of the SDGs to explicitly include both human and state security as distinct goals. This restructuring involves the introduction of a causal diagram to illustrate the interconnectedness of security with other SDG areas. Finally, we examine the specific cases of food security and climate change within the framework of our proposed causal diagram. Through these examples, we demonstrate the interdependence of various SDGs, further highlighting the crucial role of security in achieving sustainable development.

I-Theoretical Perspective: development and security nexus

The concept of "development" emerged historically as a response to the negative consequences of capitalism, particularly the need to mitigate the disruptions caused by industrialization and maintain social order (Cowen and Shenton 2010, 27).

This inherent link between development and security became even more pronounced during and after the Cold War. Western aid to underdeveloped nations often prioritized the security of Western powers rather than focusing on the security and well-being of the people in those countries.

Scholars have explored the relationship between security and development through various levels of analysis. Tschirgi et al. (2010, 48), for instance, distinguish between the individual, national, and international levels. During the Cold War, a clear distinction existed at the international level between development, focused on domestic socio-economic issues, and security policies, concerned with inter-state political and military matters. However, since the end of the Cold War, security and development concerns have become increasingly intertwined at both international and global levels (Chandler 2007, 362). This period also witnessed the "securitization" of development, shaping the current understanding of the security-development nexus. This nexus represents a set of interconnected goals and strategies for achieving both security and development (Hettne 2010, 44).

The UNDP's introduction of "human security" in 1994 marked a pivotal moment in redefining security and its relationship with development. As Kaldor (2012) notes, the 1994 Human Development Report aimed to leverage the concept of security to underscore the urgent need for development. The UNDP highlighted the contrasting security needs of individuals and states (Hettne 2010, 34), arguing that human security encompasses more than just the absence of conflict. This broadened the understanding of security from a state-centric focus to a more proactive, individual-centric approach. However, despite its appeal, the concept of human security has been criticized for its lack of clarity and analytical precision (Newman 2004). Interpretations vary, with some proponents focusing narrowly on threats of violence, while others embrace a broader definition that includes vulnerabilities like natural disasters and famine (Klingebiel 2006, 1-2). This broader interpretation positions human security as an expansive concept encompassing both traditional and non-traditional security concerns (Tsai 2009).[1]

Thus, with the introduction of human security, some scholarly studies defend the argument that human and state security are mostly intertwined. Barnett and Adger (2007) explain how human insecurity increases the risk of conflict. They suggest that any risk to national security may be both a cause and a consequence of human insecurity. For example, UN Secretary-General Kofi Annan, in his speech in 2004, claimed that people in rich countries would become more secure when their governments help underdeveloped countries defeat poverty and disease (UN 2004, vii). In other words, the security of populations in the Global South can have direct implications for the national

[1] For example, the UN (2003, 3) claims that the concept encompasses "human rights, good governance, access to education and health care, ensuring that each individual has opportunities and choices to fulfill his or her own potential".

security of countries in the Global North. This interconnectedness was emphasized in the context of the Millennium Development Goals, highlighting the nexus between human security, state security, and development. The comprehensive nature of human security has reinvigorated discussions on the link between security and development, with the concept gaining widespread use among development and security organizations globally (Walton and Johnstone 2023, 4).

In the aftermath of the 9/11 attacks, underdevelopment has been reconstructed as a security issue (Tschirgi *et al.* 2010, 48) and sustainable development has been portrayed as a requirement to avert conflict (Dalby 2019, 117). Floyd and Matthews (2013) underlined the significance of "policy innovations that might facilitate peaceful cooperation and ameliorate economic shortages and difficulties that might cause various forms of insecurity." During this period, fragile states, civil wars and terrorism have been seen as direct threats to the well-being and security of Western countries (Tschirgi *et al.* 2010, 50). For example, the EU, in its Security Strategy, states that security is the first condition for development. When formulating its security policies, the EU explicitly referenced poverty reduction and cited this as a significant tool for fighting terrorism (European Council 2003, 2).

In the following decade, by the 2010s, with the rise of a post-interventionist approach, the nexus between development and security seemed to break down. The stabilization agenda requires that the Global South should secure itself. Northern countries, in turn, assist them in doing so through a limited role rather than being directly involved in the stabilization process (Walton and Johnstone 2023, 2). In this regard, De Simone and Iocchi (2022) argue that the security-development nexus, a product of the 1990s liberal peacebuilding consensus, has come to an end.

Historical analysis reveals that the relationship between security and development is dynamic and influenced by context. A multi-dimensional theoretical framework is necessary to grasp this complexity and translate it into effective action. While the specific nature of the security-development nexus may shift over time, the fundamental interdependence of these two elements remains constant.

Spear and Williams (2012, 21) propose several ways of framing the relationship between security and development. One view sees it as a zero-sum game, where prioritizing one inevitably undermines the other. Another perspective suggests a positive-sum relationship, where security and development are mutually reinforcing, as articulated by former UN Secretary-General Kofi Annan (UN 2005). A third approach posits a hierarchical relationship, with security concerns dominating development initiatives.

This paper adopts a positive-sum approach. According to this approach, security and development are not mutually exclusive, but rather complementary and reinforcing. This means that investments in one area can lead to gains in the other. Thus, a holistic

approach that addresses both development and security concerns is more likely to achieve lasting peace and security. This framework highlights why integrating security into the SDGs is essential. The following section analyzes the existing SDGs and demonstrates the need for explicitly incorporating security into this framework.

II-Sustainable Development Goals (SDGs) and Security

Sustainable development is an inclusive objective to continuously improve the quality of life and well-being on Earth while considering the ability of future generations to meet their own needs. While the concept of sustainable development gained widespread recognition with the 1987 UN World Commission on Environment and Development report, the term itself had already begun circulating within academic circles in the 1980s. By the 1990s, discussions differentiating economic growth from development fuelled the emergence of new approaches to economic development that prioritized sustainability. This change stemmed from recognizing that development goes beyond simply increasing the economic output, which is today represented by the Gross Domestic Product (GDP) indicator obtained by expressing values of all goods and services produced in a given year, described in terms of a base period. The European Union (EU) has stressed that GDP has inherent limitations by design and purpose as a measure of development in its report on 'GDP and beyond' (European Commission 2009). Specifically, GDP fails to account for crucial factors like environmental sustainability and social inclusion despite its widespread use in policy analysis and its historical status as a leading indicator of macroeconomic activity. Similarly, the UN explored the complex relationship between economic growth and development in the Human Development Report 1996 and introduced the concept of human development. On the other hand, economic growth has been treated as part of the whole in defining development rather than playing an overarching role. The World Bank's Voices of the Poor: Can Anyone Hear Us? (Narayan et al. 2000) is one of the most comprehensive studies contributing to the literature on the shifting definition of development and one of the central policy actors undertaken for the World Development Report to gather the views of more than 60,000 people who experienced poverty. The project delves into the experiences of the poor through questions such as "How do poor people view poverty and well-being? What are their problems and priorities?" The results point out that, beyond income, people define poverty based on a range of factors, highlighting its multidimensional nature. However, the key finding of the study is that the majority of people's priority is security: food security, family security, home security, land, and inheritance (Narayan et al. 2000).

Data availability, computational and methodological developments, and the demand for national and international policy play an efficient role in the dynamic improvement of the development concept. Sen's (2000) capability approach expressing the basis of the multidimensional aspect of poverty has also contributed to defining poverty and

development. The UNDP proposed the Human Development Index (HDI), which hinges on the capability approach, as a measure that extends beyond GDP by including income, health, and education in the definition (Decancq and Schokkaert 2016, 22). Following Sen's capability approach, the Oxford Poverty and Human Development Initiative (OPHI) has developed the Global Multidimensional Poverty Index (MPI) to capture the multidimensional aspect of poverty in developing countries, just as the need to collect more information for measuring development. Thus, development and security have intertwined over time due to the dynamic development structure by intersecting at the human denominator (Bilgen 2017, 29).

The UN General Assembly (2015) adopted the Sustainable Development Goals (SDGs) entitled "Transforming our world: the 2030 Agenda for Sustainable Development" in 2015 as an extended version of the Millennium Development Goals. The SDGs are listed to eradicate extreme poverty and hunger; to achieve universal primary education; promote gender equality; reduce child mortality; improve maternal health; combat HIV/AIDS, malaria, and other diseases; ensure environmental sustainability; to develop a global partnership for development.

The Sustainable Development Goals (SDGs) comprise 17 interconnected goals aimed at creating a better world by 2030. These goals encompass a wide range of aspirations, from ending poverty and hunger to promoting health, education, and gender equality.[2] The proposed diagram draws heavily on the mutual relationship between security and development. Our causal diagram visually reinforces the reciprocity of security and development, demonstrating that security and development are interconnected. As seen in Figure 1, a causal diagram can also demonstrate the intercorrelation among the goals. The most salient feature of these goals is that any development in one of the goals affects others.

[2] All the goals and their specific targets are detailed on the UN website: https://sdgs.un.org/goals. For instance, Goal 2 covers achieving food security, improving nutrition and promoting sustainable agriculture.

In our proposed causal diagram, we restructure the SDGs by introducing "security" as "Goal 0." While the concept of security is not explicitly mentioned within the current SDGs (except within Goal 2 on food security), Goal 16, which focuses on peace, justice, and strong institutions, touches upon human rights and the importance of independent human rights institutions. It acknowledges the interconnectedness of human rights, peace, security, and development, which partially supports our argument. Crucially, we designate security as "Goal 0" because it underpins all other goals. Whether at the individual or state level, the ultimate aim of addressing development challenges is to achieve security and peace. Security is the foundation upon which all other aspirations for sustainable development rest.

The absence of a dedicated security goal within the SDGs and the lack of explicit recognition of the interconnectedness of state and human security

present a significant challenge for policy implementation. To address this, we propose positioning security at the heart of the sustainable development agenda. This means recognizing that progress (or setbacks) across all 17 SDGs will have ripple effects on both state and human security and, ultimately, on development itself.

Inspired by Goldstein (2016), we advocate for a solution-oriented approach. To effectively advance the SDG agenda, we must re-examine these goals through a multi-dimensional lens that acknowledges the dynamic interplay between development and security. This requires moving beyond traditional interpretations of these concepts. By doing so, we call for a shift from a focus on sustainable development goals to a broader vision of sustainable security for all.

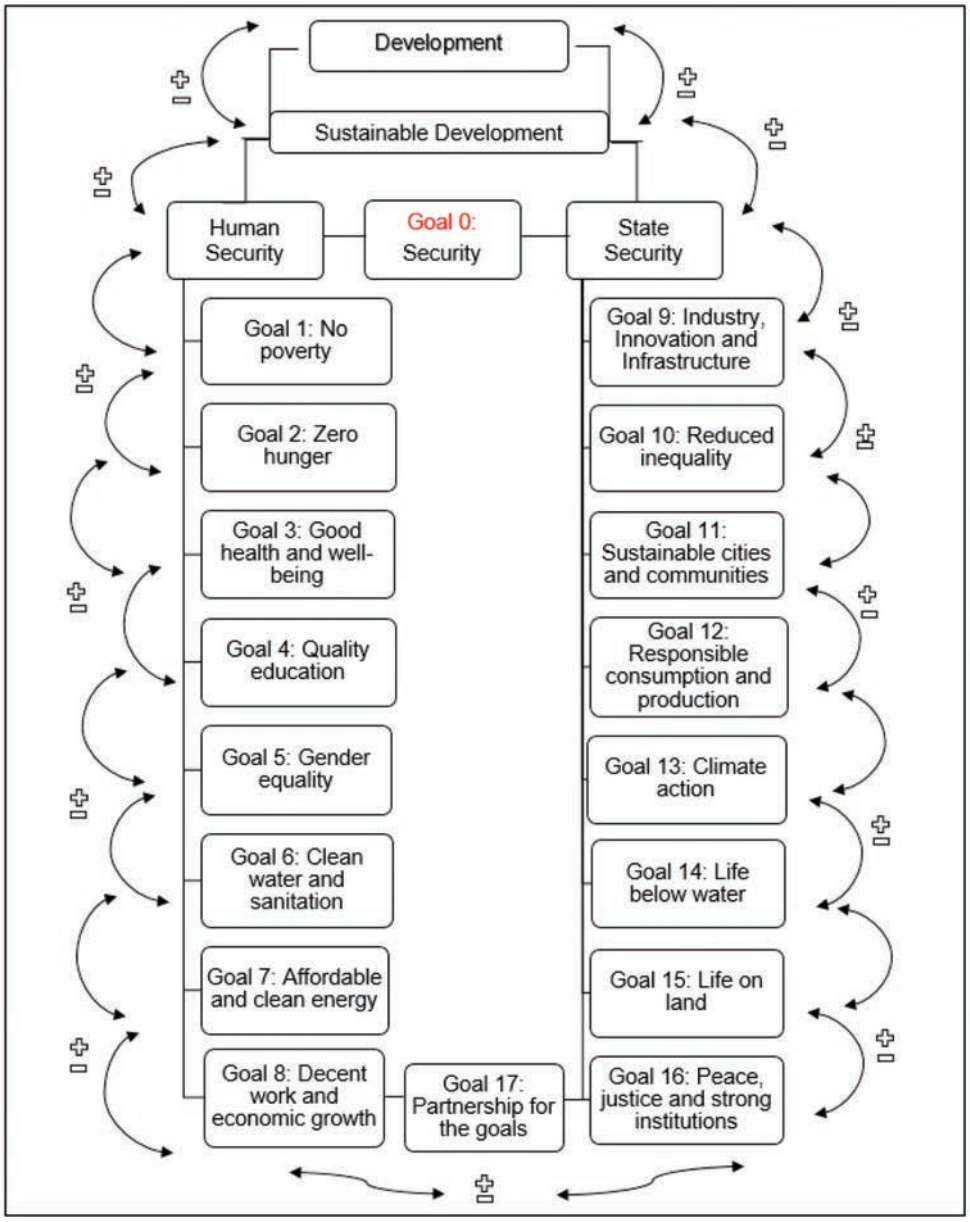


Figure 1 Causal diagram for sustainable development goals
Source: own preparation

Furthermore, in Figure 1, we try to recast SDGs as a global security issue and reserve separate places for state and human security in the diagram. From this point of view, in the following section, we look closer to this argument with two different but connected cases, climate change, and food security, in correlation with human and state security, which will also help us understand why we divide the security as human and state within the SDGs.

III-Food Security, Climate Change as SDGs and security-development nexus

While food security and climate change appear as separate goals within the SDGs, their interconnectedness highlights the inherent link between development and security. As two of the most pressing issues facing our world, their analysis reveals a cascading effect with implications for global security. This underscores the necessity of integrating both traditional and human security dimensions within the SDGs framework. Figure 2 illustrates the intricate relationship among development, security, climate change, and food insecurity, providing a visual representation of this complex nexus.

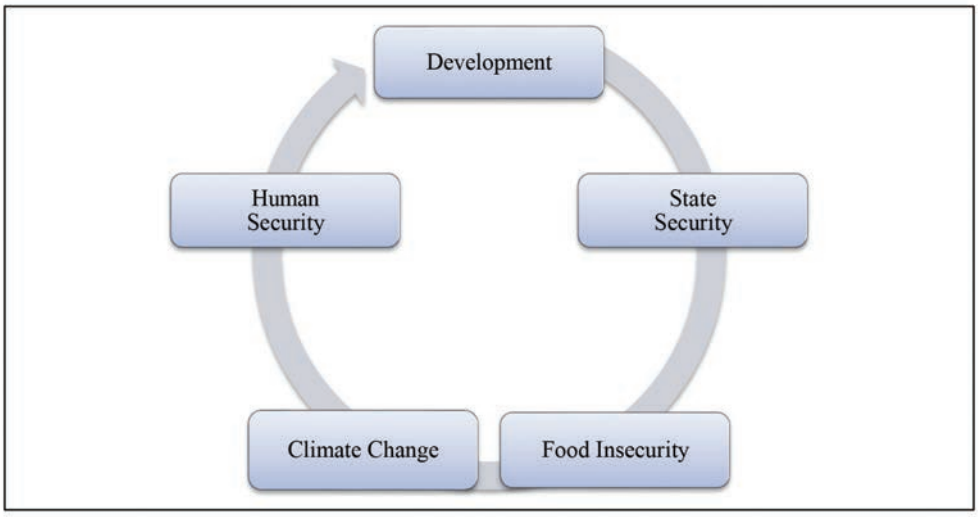


Figure 2 The interlink of development, human and state security, climate change, and food security
Source: own preparation

Food security, enshrined in SDG 2 (Zero Hunger), is defined by the Food and Agriculture Organization (FAO) (2009) as access to sufficient, safe, and nutritious food—physically, socially, and economically—to support an active and healthy life. While primarily associated with human security and development, food insecurity has profound implications for state security as well.

For developed countries, food insecurity in the Global South can trigger mass migration, posing potential challenges related to integration and identity. Furthermore, competition for scarce resources exacerbated by food insecurity can

fuel internal and external conflicts. As Busby (2018) notes, factors like agriculture, food prices, economic growth, migration, and disasters can mediate conflict. The link between food security and national security is increasingly recognized, exemplified by the World Food Programme's 2020 Nobel Peace Prize for its efforts in combating hunger and fostering peace in conflict zones.

The UN General Assembly (2015) places climate change as a distinguished title within SDGs in Goal 13. The UN (n.d) defines climate change as "the long-term shifts in temperatures and weather patterns arising from natural causes such as sun's activity or volcanic eruptions and from human activity, which is the primary driver of climate change." However, high temperatures are not the one fact of climate change since the Earth has an interrelated system where any changes in one area can influence all the other changes in others, such as droughts, water scarcity, rising sea levels, flooding, storms, melting polar ice (Garcia 2010).

The relationship between climate change and security is complex and debatable. While some scholars focus on climate change's potential to exacerbate violent conflict (Busby 2018), the link is not universally accepted. However, there is growing recognition of climate change's impact on state wealth, economic growth, and human security, highlighting the interconnectedness of climate, development, and security (Richards 2023).

The International Panel on Climate Change (IPCC) advocates for a comprehensive approach that integrates these three elements, prioritizing development policies to mitigate climate change's adverse security impacts. This relationship is inherently interconnected and development and security are mutually reinforcing, with each dependent on the other, particularly in the context of climate change. Climate-related insecurities directly hinder sustainable development.

Integrating security into the SDGs framework offers several advantages. It can facilitate policies to reduce the environmental impact of conflict, currently an under-recognized issue. Furthermore, it can amplify the voices of vulnerable nations, like those in the Pacific Islands Forum, facing existential threats from climate change. As Richards (2023) observes, the current SDGs framework fails to adequately address the unique environmental hazards confronting these countries.

The interconnectedness of the SDGs is further exemplified by the intersection of climate change and food security, with significant implications for both human and state security. As previously noted, progress in one SDG influences others, creating a ripple effect across the entire framework. Climate change, as highlighted by Spratt and Dunlop (2019), already threatens food security through drought, crop yield decline, and rising food prices, particularly in vulnerable regions like the Middle East, Maghreb, and Sahel. Dupont and Pearman (2006) emphasize the direct link between climate change and food insecurity, citing desertification, rising sea levels,

and extreme weather events as contributing factors. This climate-induced food insecurity has far-reaching consequences. It has contributed to migration crises, as noted by Spratt and Dunlop (2019), and reinforces the notion of food security as a national security issue, especially for food-importing countries (Christensen 1977, cited in Nussio and Pernet 2013). The impact is particularly acute in regions reliant on rain-fed agriculture, like the Horn of Africa, where El Niño events have caused widespread food insecurity and drought (Parker *et al.* 2016). This vulnerability is further underscored by the heavy financial burden of food imports faced by many African nations.

Conclusion

Throughout history, the concept of development has increasingly been linked to security in discourse and at the policy level. This paper questions the controversial relationship between development and security and defends a reciprocal approach, implying that security and development are preconditions for each other. After implementing the mutual characteristic of the relationship between development and security, the paper makes a policy recommendation and suggests introducing security into the causal diagram of SDGs by labelling it "SDG number zero". The number zero of SDGs, security, is placed at the top of the diagram to avoid the emergence of war, violence, and conflict by addressing structural-developmental root causes. Furthermore, the causal diagram positions security as "Goal 0" at the top to signify its foundational role within the goals and to emphasize it as a multidimensional concept covering the other 17 goals. Progress on any SDGs strengthens the foundation of a stable and secure environment. Conversely, failing to progress on any of these goals can lead to heightened social tensions and potential conflict, thereby jeopardizing security.

The paper concludes that the shortcomings at the policy level can be compounded by incorporating the concept of security -with both dimensions of human and state security- in SDGs. In their search for solutions to global problems, global actors explicitly or implicitly address the security-development spectrum. However, there is a gap between policy rhetoric and reality. Incorporating security within the SDGs may act as a solution for filling this gap. Especially as international institutions and organizations acting within the domains of security and development are highly fragmented and operate in isolation from each other. The incorporation of human and state security into SDGs and the proposition of a causal diagram have the potential to strengthen the collaboration among different actors with different professionalisms. Thus, incorporating security in SDGs is instrumental in bringing a comprehensive approach at the practical level. Integrating security in SDGs suggests a way to reach beyond the traditional choice between "development strategies" or "military and intelligence organizations" as solutions. In the long run, the passage from sustainable development to sustainable security after incorporating human and state security dimensions in SDGs becomes the primary objective at the policy level.

In conclusion, the explicit securitization of SDGs may offer an essential alternative policy option. Put differently, the balance between security and development must be reorganized in favour of security and at the expense of development. The incorporation of security into SDGs may act as a catalyst for accelerating efforts toward the securitization of SDGs, which is a requirement *per se* under the adverse conditions accelerated by climate change and food security, among many others.

References

Barnett, Jon, and W. Neil Adger. 2007. "Climate Change, Human Security and Violent Conflict." *Political Geography* 26 (6): 639-655. DOI: 10.1016/j.polgeo.2007.03.003

Beall Jo, Thomas Goodfellow, and James Putzel. 2006. "Introductory article: on the discourse of terrorism, security and development." *Journal of International Development* 18: 51–67. DOI: 10.1002/jid.1262

Bilgen, Arda. 2017. "Güvenliksiz Kalkınma, Kalkınmasız Güvenlik Mümkün mü? Güvenlik-Kalkınma İlişkisinin Dönüşüm Süreci ve Farklı Yaklaşımlarla Kavramsallaştırılması." Uluslararası İlişkiler 14 (55): 19-40. https://doi.org/10.33458/uidergisi.513497

Busby, Joshua. 2018. "Taking Stock: The Field of Climate and Security." *Current Climate Change Reports* 4: 338-346. https://doi.org/10.1007/s40641-018-0116-z

Buzan Barry, Ole Waever, and Jaap De Wilde. 1998. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner.

Chandler, David. 2007. "The Security-Development Nexus and the Rise of 'anti-foreign policy'." *Journal of International Relations and Development* 10: 362-286. DOI: https://doi.org/10.1057/palgrave.jird.1800135

Cilliers, Jakkie. 2006. "New Interfaces Between Security and Development." In New Interfaces Between Security and Development. Changing Concepts and Approaches, edited by Stephan Klingebiel. Bonn: Deutsches Institut für Entwicklungspolitik GmbH. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-308068

Cowen, Michael, and Robert Shenton. 2010. "The Invention of Development." In Development Ethics. Edited by Des Gasper. London: Routledge.

Dalby, Simon. 2019. Climate change, security, and sustainability. 1st ed. Routledge: London.

De Simone, Sara, and Alessio Iocchi. 2022. "The End of the Security-Development Nexus? Reflections from Counterinsurgency in North-Eastern Nigeria." *Third World Quarterly* 43 (12): 2757-2774. DOI: 10.1080/01436597.2022.2104705

Decancq, Koen, and Erik Schokkaert. 2016. "Beyond GDP: Using equivalent incomes to measure well-being in Europe." *Social Indicators Research* 126 (1): 21-55. http://dx.doi.org/10.1007/s11205-015-0885-x

Dupont, Alan, and Graeme Pearman. 2006. "Heating up the planet, climate change and security". Lowy Institute Paper 12. https://www.files.ethz.ch/isn/87076/2006-06-13.pdf

Duffield, Mark. 2017. "Human Security and the Development-Security Nexus. An historical overview". *Ragion pratica,* Rivista semestrale 1: 61-76. DOI: 10.1415/86437

European Commission. 2009. GDP and beyond: Measuring progress in a changing world. Brussels: European Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0433

European Council. 2003. A Secure Europe in a Better World: A European Security Strategy. Brussels: European Union. https://www.consilium.europa.eu/en/documents-publications/publications/european-security-strategy-secure-europe-better-world/

Food and Agriculture Organization (FAO). 2009. The State of Food Insecurity in the World- Economic crises – impacts and lessons learned. https://www.fao.org/3/i0876e/i0876e00.htm

Floyd Rita and Richard A. Matthew (ed.). 2013. Environmental Security: Approaches and Issues. London: Routledge.

Garcia, Denise. 2010. "The climate security divide: Bridging human and national security in Africa". *African Security Review* 17(3): 2-17. DOI: 10.1080/10246029.2008.9627480

Goldstein Joshua S. 2016. "Climate Change as a Global Security Issue". *Journal of Global Security Studies* 1(1): 95-98. DOI: 10.1093/jogss/ogv010

Guterres, Antonio. 2016. Secretary-General-designate Antonio Guterres' remarks to the General Assembly upon taking the oath of office. https://www.un.org/sg/en/content/sg/speeches/2016-12-12/secretary-general-designate-ant%C3%B3nio-guterres-oath-office-speech

__. 2017. Repositioning the UN development system to deliver on the 2030 Agenda: Ensuring a better future for all. https://digitallibrary.un.org/record/1298793?ln=en

__. 2018. Peacebuilding and sustaining peace: Report of the Secretary-General. https://reliefweb.int/sites/reliefweb.int/files/resources/SG%20report%20on%20peacebuilding%20and%20sustaining%20peace.As%20issued.A-72-707-S-2018-43.E.pdf

Hettne, Bjorn. 2010. "Development and Security: Origins and Future". *Security Dialogue* 41(1): pp. 31–52. http://www.jstor.org/stable/26301184

Kaldor, Mary. 2012. "Human Security in Complex Operations". *Prism* 2(2): 3-15. http://eprints.lse.ac.uk/id/eprint/49494

Khagram, Sanjeev, William C. Clark and Dana Firas Raad, 2003. "From the Environment and Human Security to Sustainable Security and Development". Journal of Human Development 4(2): 289-313. DOI: 10.1080/1464988032000087604

Klingebiel, Stephan (Ed.) 2006. "Introduction". In New interfaces between security and development: changing concepts and approaches, Studies (no. 13), Edited by Stephan Klingebiel. Deutsches Institut für Entwicklungspolitik (DIE), Bonn. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2419373

Keukeleire Stephan and Kolja Raube. 2013. "The security-development nexus and securitization in the EU's policies towards developing countries." *Cambridge Review of International Affairs* 26 (3): 556–57.

Lamont, Clare. 2015. Research Methods in International Relations. Sage Publications.

Narayan, Deepa, Raj Patel, Kai Schafft, Rademacher. 2000. Can Anyone Hear Us?: Voices of the Poor. New York: Oxford University Press.

Newman, Edward. 2004. "A Normatively Attractive but Analytically Weak Concept". *Security Dialogue* 35(3): 358-359. https://doi.org/10.1177/096701060403500316

Nussio, Enzo, and Corinne A. Pernet. 2013. "The Securitization of Food Security in Columbia, 1970-2010." *Journal of Latin American Studies* 45 (4): 641-668. DOI: 10.1017/S0022216X1300117X

Parker, Helen, Naomi Oates, Nathaniel Mason, Roger Calow, William Chadza, Eva Ludi. 2016. "Gender, agriculture and water insecurity". Overseas Development Institute (ODI) Insights, London.

Richards, Imogen. 2023. "Capturing the environment, security, and development nexus: intergovernmental and NGO programming during the climate crisis". *Conflict, Security & Development* 23 (5): 425-445. DOI: 10.1080/14678802.2023.2211019

Sen, Amartya. 2000. Development as Freedom. 1st Edition. New York: Anchor Books Edition.

Spear, Joanna and Peter D. Williams. 2012. Security and Development in Global Politics, A Critical Comparison. Georgetown University Press.

Spratt, David and Ian Dunlop. 2019. "Existential climate-related security risk." Breakthrough - National Centre for Climate Restoration. https://docs.wixstatic.com/ugd/148cb0_90dc2a2637f348edae45943a88da04d4.pd

Stern, Maria, and Joakim Öjendal. 2010. "Mapping the Security-Development Nexus: Conflict, Complexity, Cacophony, Convergence." *Security Dialogue* 41 (1): 5-29. https://doi.org/10.1177/09670106093570

Stewart, Frances. 2013. "Federalism, Decentralisation, and Horizontal Inequalities." *Centre for Research on Inequality, Human Security and Ethnicity, CRISE* (no. 3). https://assets.publishing.service.gov.uk/media/57a08b06e5274a27b20008eb/policybriefing3.pdf

Tsai, Yu-tai. 2009. "The Emergence of Human Security: A Constructivist View." *International Journal of Peace Studies* 14 (2): 19-33. https://www.jstor.org/stable/41852991

Tschirgi, Necla, Michael S. Lund, Francesco Mancini (eds). 2010. The Security Development Nexus. Security and Development: Searching for Critical Connections. Lynne Rienner: Boulder CO USA.

The United Nations (UN). 2003. "Human Security Now, Final Report of the Commission on Human Security", New York: United Nations Publications. https://digitallibrary.un.org/record/503749

The United Nations (UN). 2004. "A More Secure World: Our Shared Responsibility, Report of the Secretary-General's High-Level Panel on Threats, Challenges and Change". New York: United Nations Publications. https://www.un.org/peacebuilding/sites/www.un.org.peacebuilding/files/documents/hlp_more_secure_world.pdf

The United Nations (UN). 2005. "Secretary General: In larger freedom: towards development, security, and human rights for all, report of the Secretary General". New York: United Nations Oublications. https://digitallibrary.un.org/record/550204.

The United Nations (UN). n.d. "What is climate change?". https://www.un.org/en/climatechange/what-is-climate-change.

The United Nations General Assembly. 2015. "Transforming Our World: the 2030 Agenda for Sustainable Development". Resolution 70/1. https://documents.un.org/doc/undoc/gen/n15/291/89/pdf/n1529189.pdf

Walton, Oliver, and Andrew Johnstone. 2023. "The Fragmentation of the security and development nexus: the UK government's approach to security and development 2015-2022." *Peacebuilding* 12 (3): 429-444. https://doi.org/10.1080/21647259.2023.2291920

Competing Interests

The authors have no competing interest to declare.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Evolution of warships in the digital age

Commander (Navy) Alexandru-Lucian CUCINSCHI, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: cucinschi.alexandru@gmail.com

Abstract

In the context of historical developments in maritime conflicts, warships have always been the central pillars of naval power, determining the course of empires and influencing the outcomes of wars. From ancient Greek triremes and Roman galleys to modern aircraft carriers, these vessels have been essential in both national defence and the exploration and colonization of new territories. In contemporary times, the role of warships has further expanded to include humanitarian and peacekeeping missions while maintaining their fundamental functions of protecting maritime communication routes, controlling maritime spaces, and projecting force. As technology continues to advance, the digital age redefines naval capabilities, propelling warships into a new era of innovation and strategic complexity. This article provides a brief history of warships, highlighting the essential elements that have contributed to their development and ongoing relevance, and explores the future impact of the digital age on these crucial platforms for global security.

Keywords:

maritime power; maritime security; digital age; warships;
digital technology; artificial intelligence.

Article info
Received: 20 September 2024; Revised: 17 October 2024; Accepted: 11 November 2024; Available online: 17 January 2025

Citation: Cucinschi, A.L. 2024. "Evolution of warships in the digital age".
Bulletin of "Carol I" National Defence University, 13(4): 37-45. https://doi.org/10.53477/2284-9378-24-47

This article explores the main historical milestones that have defined the functions and importance of warships over time, highlighting the way in which they have retained their essential missions despite the transformations brought by technological progress. It also analyzes the implications of modernization and digitalization on contemporary naval operations, underscoring emerging challenges and opportunities within global maritime security. This critical analysis aims to provide a comprehensive understanding of the historical and technological dynamics of warships, highlighting their ongoing relevance in the current geopolitical context. Through this historical and contemporary lens, the study of warships reveals not only a tale of adaptation and innovation but also a continuous manifestation of their lasting influence on geopolitics and international security.

In an ever-changing world, naval forces will continue to play a central role, adapting to new technological and strategic realities.
The research methodology for this article includes:

- a chronological approach to examine key transitions in the design and function of warships, identifying the technological and geopolitical factors that have driven these changes;
- the selection and analysis of case studies of nations that have made significant contributions to naval innovations, such as England in the early modern period or the United States in the contemporary era, to understand variations in strategies and technologies;
- an analysis of how these technological and historical developments influence national and international defense strategies, using strategic models and scenarios from current conflicts.

The research limitations are represented by the lack of access to classified information about the latest technologies implemented by naval forces belonging to states with highly developed defence industries, in which military institutions have research and innovation institutes. In most states today, armed forces no longer innovate; they focus on selecting and developing civilian technologies that have military relevance.
The article is structured into four parts: the first part presents some historical milestones relevant to the evolution of warships; the second part outlines a possible model for building naval capabilities to understand mainly the limitations of naval platforms; and in the third and fourth parts, the main characteristics of the digital age and its impact on warships are presented.

A brief history of warships

Throughout history, warships have been essential instruments of maritime power, influencing the course of conflicts and the formation of empires. In the modern era, the missions of warships are primarily those consolidated over the centuries, playing a crucial role in global maritime security, protecting communication lines, and projecting force in regional and international conflicts.

To highlight the fact that the missions of warships have not fundamentally changed and to construct a pattern of their evolution and relevance, I will present the main historical milestones that have defined warships and their importance.
The first warships, such as Greek triremes and Roman galleys, were powered by oars and used in maritime confrontations. These ships were built for rapid manoeuvrability and their purpose was to inflict damage through boarding, utilizing archers and catapults on board (Strauss 2004).

In the Middle Ages, the Vikings developed long, fast, and manoeuvrable ships used for raiding and trade (Magnusson 1980). These ships influenced the later design of warships in Europe.
Advancements in shipbuilding led to the emergence of line ships, large heavily armed vessels that dominated the seas. These ships had multiple decks equipped with cannons, used in major naval battles, such as those during the Napoleonic Wars.

Warships facilitated the exploration and colonization of new territories. During the Age of Discovery, nations such as Portugal, Spain, the Netherlands, and England used warships to explore unknown lands, establish colonies, and claim new territories. This expansion contributed to the creation of global empires and the spread of cultural and economic influences.
Control of the seas and oceans was essential for the economic prosperity of empires. Warships protected trade routes against piracy and enemy attacks, ensuring the free flow of goods and resources. For example, as the British Empire expanded, the Royal Navy protected global trade routes, contributing to Britain's economic dominance in the 17th to 19th centuries.

The Industrial Revolution marked the transition from sailing ships to steam propulsion. This era introduced armoured warships, such as the famous HMS Warrior.
The two World Wars led to rapid developments in warships. Battleships like the HMS Dreadnought redefined naval warfare in the early 20th century (Edwards 2024). After World War II, aircraft carriers became essential due to their capacity to launch aircraft and project power over great distances.

The presence of a strong fleet can act as a deterrent against rivals and can be used to project a nation's power on an international scale. Warships enable the rapid and strategic deployment of military forces, providing nations with the ability to intervene in conflicts far from their borders. These capabilities are evident in modern examples of aircraft carriers and maritime strike groups employed by the world's great powers.
Famous naval battles, such as the Battle of Midway, demonstrated that naval superiority can determine the fate of wars and change the international balance of power (history.com 2024). Victory in these confrontations granted maritime powers control over the seas, undermining the ability of enemies to defend or expand territories.

In the contemporary era, warships are not only instruments of war, but also platforms for humanitarian missions, peacekeeping, and international cooperation. Participation in international maritime exercises and joint missions helps strengthen relationships between nations, promoting global stability and security.
Moving forward, I believe that detailing how naval capabilities are constructed is necessary, considering their diversity and specificity depending on the factors that are determinants of the main characteristics of a naval platform.

Factors that influence the shipbuilding – types of ships

To understand the elements that contribute to building the capabilities of naval forces, I believe that the elements derived from the study I conducted regarding coastal warfare can serve as a simplistic model upon which naval platforms are built to suit various strategic situations.
Thus, the main conclusion of the study, based on the analysis of historical cases of military actions conducted in the coastal area, is that the characteristics of the environment influence the way in which the naval platform is constructed, which, in turn, affects the weapons and technology installed on the platform, all of them having direct implications on the tactics used in combat (Cucinschi 2020).

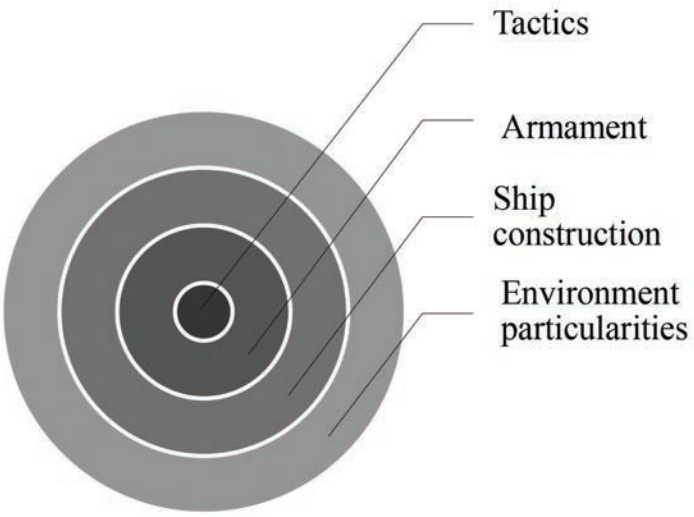


Figure 1 The interdependence between the main elements of littoral warfare (Cucinschi 2020)

Subsequently, through case studies focused on states that have developed effective capabilities for coastal warfare, I have concluded that, in addition to the previously mentioned factors, consideration must also be given to the adversary, the form of action (offensive or defensive, and less so in the case of stability operations), and experience in building naval platforms (Cucinschi 2020).

Building on this study, one can understand how naval capabilities are currently constructed based on the physical environment—this

may allow for the construction of large platforms (for oceans and large seas) or small ones, for smaller, enclosed, or semi-enclosed seas. Subsequently, the platforms, depending on their sizes, can be equipped with different types of armaments. Given that naval forces address combat in environments such as surface, anti-submarine, and air defence (more recently, seabed warfare), the weaponry is grouped within these three categories.

Typically, relatively small ships, such as corvettes, allow for the equipping of weaponry and sensors for combat in a single environment, while being limited in the others. Frigates, which are medium-sized ships, allow for the equipping of sensors and weaponry for combat in two environments, with limitations in the third. Destroyers, being large ships, allow for the installation of equipment and sensors capable of fighting in all three environments.
In addition to specific missions only for naval forces, military vessels can also carry out actions in support of ground forces, air forces, and special operations forces, usually with large ships (destroyers, cruisers, aircraft carriers) or specialized vessels (assault ships).

Up to now, seabed warfare has not been associated with a specific type of ship, as there are no concrete elements about how to approach this new environment.
I believe it is important to understand how the main types of warships are constructed because, in many cases, the expectations of other force categories or the commanders of combined forces exceed the realm of possibility for naval platforms.

Additionally, to understand how the digital age impacts the transformation of military vessels, it is necessary to understand the benchmarks that underlie the specificity of the types of ships used in current conflicts, which is why I have conducted this brief analysis.
Next, I will carry out an analysis concerning the transition into the digital age and the fact that it can lead to transformations regarding the building of capabilities for naval force platforms.

Digital age – defining characteristics

The digital age, often referred to as the information age, is a period in human history characterized by major technological revolutions and the transition from a resource-based economy to one based on information and knowledge. This era features several defining characteristics that have profoundly transformed society, economy, culture, and the way we interact with one another.

1. *Digital Technology and Information Accessibility:* One of the most emblematic traits of the digital age is the abundance and accessibility of information through technology. The internet, personal computers, smartphones, and other digital devices enable us to access and distribute information on a global scale in a fast and efficient manner. This unlimited

access to information has democratized knowledge, allowing individuals to learn and grow autonomously (Katz and Ronald 2002).

2. Global Communications: The digital age has radically transformed the way we communicate. Social networks, emails, instant messaging, and video conferencing platforms allow us to stay connected with others, regardless of geographical distances. This globalization of communication has facilitated cultural and economic exchanges but has also led to phenomena such as technology dependence and the rapid spread of misinformation (Castells 1996).

3. Digital Economy: Technological innovations have led to the emergence of a digital economy, where goods and services are created, managed, and traded online. E-commerce platforms, digital assets, and cryptocurrencies are manifestations of this transition. The digital economy has created new business opportunities and changed employment paradigms, enabling remote work and the development of careers in emerging fields (Brynjolfsson and McAfee 2014).

4. Automation and Artificial Intelligence: Advances in artificial intelligence and automation have had a profound impact on jobs and industrial efficiency. While these technologies have improved productivity and reduced costs, they have also raised concerns regarding job loss and ethics in the use of AI (Tapscott 1995).

5. Social and Cultural Impact: The digital age has deeply shaped the social and cultural aspects of our lives. Individuals build hybrid identities, both physical and virtual, with the ability to express themselves and organize into digital communities. However, this environment has also contributed to social isolation and raised questions regarding privacy and the security of personal data (Turkle 2012).

6. Security Challenges: With the benefits of digital connectivity come challenges related to cybersecurity. Threats such as hacking, online fraud, and cyberattacks are on the rise, necessitating the need for sophisticated security solutions and education in data protection (Van Dijk 2012).

In conclusion, the digital age is characterized by increased interconnectedness, economic and technological innovations, and social and ethical challenges. These transformations have led to a reconfiguration of global society, providing numerous opportunities while simultaneously demanding responsibility in managing the technological impacts on humanity.

The impact of the digital age on naval platforms

The digital age has brought significant transformations across multiple fields, including maritime conflict. Warships, considered essential in the defence strategies of any maritime nation, have not remained unaffected by these changes.

First of all, digital technology has revolutionized the equipment and onboard systems

of warships. The information management systems aboard ships have become more advanced and interconnected. The integration of digital technologies has led to the development of more efficient sensor systems, secure communication systems, and improved rapid response capabilities. For instance, the use of artificial intelligence has enabled the automation of complex processes, allowing many routine operations to be managed with minimal impact from the human crew, thereby reducing errors and increasing operational efficiency.

Secondly, the digital age has opened new horizons regarding naval strategies. The concept of cyber warfare has become a crucial component of modern conflicts. Warships must now be prepared for cyber threats, developing both defensive and offensive digital capabilities. This entails implementing advanced cybersecurity systems and training personnel in cyber warfare, ensuring the protection of critical information and communication infrastructure.

Furthermore, computer-aided design and virtual simulations have revolutionized how warships are conceived and tested. These technologies allow engineers to create highly detailed 3D models and simulate various operational scenarios before actual construction begins. As a result, design errors are minimized, and the ship's performance is optimized for different combat conditions, saving significant time and resources.

Additionally, modern weapon systems integrated with digital technology represent a significant advancement in both defence and offence. Digitally guided technologies, such as smart torpedoes and guided missiles, offer superior precision and firepower. Anti-aircraft and anti-ship defence systems have also been greatly optimized through advanced sensors and radars, allowing threats to be detected and neutralized well before they become critical.
Moreover, digital technology has led to improvements in the durability and sustainability of warships. Modern designs focus on reducing radar and acoustic signatures, using advanced materials and innovative designs that make them harder to detect by enemies and more energy-efficient.

Furthermore, the digital age has fostered integration and interoperability between different types of armed forces and nations. Warships are now capable of participating in multinational exercises and peacekeeping operations due to standardized communication and information-sharing systems. These capabilities are crucial for international cooperation and for rapidly updating strategic information in crisis situations.
In addition to the technical and strategic advantages, the transformations of the digital age have also posed some ethical and social dilemmas. Automation and the use of artificial intelligence in combat decisions raise issues of accountability and morality, especially concerning lethal actions. Additionally, the growing reliance on digital systems exposes warships to risks of manipulation or malfunctions caused by cyberattacks.

Thus, it can be asserted that the digital age has profoundly influenced the evolution of warships, radically redefining the way they operate. Technological innovations have led to improvements in the efficiency and operational capabilities of vessels, while new strategic and ethical challenges have emerged in the context of digital integration. It is essential for naval forces to continue adapting to these changes, developing innovative solutions to meet modern defence and security requirements.

Conclusions

Throughout history, warships have remained essential in projecting maritime power and protecting international security. Although the fundamental missions of these vessels have evolved, their essence has remained the same: ensuring control of maritime space and protecting sea lines of communication.
From the era of triremes and galleys to modern ships equipped with advanced technologies, the evolution of warships reflects the progress in shipbuilding and armament. These vessels have been instrumental not only in wars but also in exploration and colonization, defining the outlines of great historical empires.

The Industrial Revolution and the digital age, more recently, have fundamentally transformed naval platforms. Modern propulsion, sophisticated armament, and automation have increased efficiency but have also introduced new challenges, such as the need for cybersecurity and the ethical management of artificial intelligence.
The digital age has facilitated the promotion of international maritime cooperation. Modern warships are equipped for interoperability, allowing participation in multinational exercises and missions, which strengthens diplomatic relations and contributes to global security.

In the context of the digital age, naval forces must continue to adapt, developing innovative solutions to address contemporary challenges. The integration of new technologies must be balanced with ethical responsibilities and protection against cyber threats.

References

Brynjolfsson, E., and A. McAfee. 2014. "The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies". W. W. Norton & Company, Inc. https://edisciplinas.usp.br/pluginfile.php/4312922/mod_resource/content/2/Erik%20-%20The%20Second%20Machine%20Age.pdf.

Castells, M. 1996. *The Rise of the Network Society.* Malden: Blackwell Publishers. https://onlinelibrary.wiley.com/doi/book/10.1002/9781444319514.

Cucinschi, Alexandru-Lucian. 2020. *Lupta la litoral pentru Forțele Navale.* București: Biblioteca Universității Naționale de Apărare, Cota D: 4623.

Edwards, Giles. 2024. "How the Dreadnought sparked the 20th Century's first arms race". https://www.bbc.com/news/magazine-27641717.

history.com. 2024. "Battle of Midway". https://www.history.com/topics/world-war-ii/battle-of-midway.

Katz, J., and R. Ronald. 2002. *Social Consequences of Internet Use: Access, Involvement, and Interaction.* MIT Press Ltd. https://direct.mit.edu/books/monograph/3803/Social-Consequences-of-Internet-UseAccess

Magnusson, Magnus. 1980. *Vikings.* E.P. Duton. https://www.abebooks.co.uk/9780370302720/Vikings-Magnusson-Magnus-0370302729/plp

Strauss, Barry. 2004. *The Battle of Salamis The Naval Encounter That Saved Greece - and Western Civilisation.* Simon and Schuster. https://books.google.ro/books/about/The_Battle_of_Salamis.html?id=gcJ34dOcA3MC&redir_esc=y.

Tapscott, D. 1995. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence.* McGraw-Hill. https://books.google.ro/books/about/The_Digital_Economy.html?id=Nzi8QgAACAAJ&redir_esc=y.

Turkle, S. 2012. "Alone Together: Why We Expect More from Technology and Less from Each Other". https://www.academia.edu/3129910/Alone_together_Why_we_expect_more_from_technology_and_less_from_each_other.

Van Dijk, J. 2012. *The Network Society.* SAGE Publications Ltd.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

New data on the practice of desertions from the Red (Soviet) Army as an expression of the anti-Soviet resistance of the Moldavian SSR population in the years 1944-1954

Assoc.prof. habil. Anatolie LEȘCU, Ph.D.*

*"Alexandru cel Bun" Military Academy of the Armed Forces, Chisinau, Republic of Moldova
e-mail: lescuanatol@yahoo.com

Abstract

The history of the eastern part of what used to be Moldova, or the eastern area of Romanian territory located in the Pruto-Nistrean interfluve, which later became known as Bessarabia, is a tragic and turbulent one. In the last 200 years alone, this territory has undergone three occupations and annexations, all carried out by the Russian state in different forms: 1812, 1940, and 1944. The Sovietization of Moldova after the subsequent occupation of Bessarabia in the summer of 1944 proceeded with great difficulties, as the artificially created population of the Moldavian SSR resisted Soviet authorities in various ways. One of the forms of resistance was desertion from the Soviet Army. Desertion, a phenomenon characteristic of all armies worldwide, is a criminal offence that involves evading military service through various methods, such as fleeing from a unit or avoiding enlistment altogether. Under the conditions of forced Sovietization in the SSR between 1944 and 1953, this practice took on distinctly anti-Soviet characteristics, becoming a part of the population's struggle against the occupiers.

Keywords:
USSR; Moldavian SSR; Red Army (Soviet); mobilization; population; desertion; security services; soldier; officer; murder; escape; arrest.

Article info
Received: 26 June 2024; Revised: 25 August 2024; Accepted: 6 November 2024; Available online: 17 January 2025

Citation: Leşcu, A. 2024. "New data on the practice of desertions from the Red (Soviet) Army as an expression of the anti-Soviet resistance of the Moldavian SSR population in the years 1944-1954." *Bulletin of "Carol I" National Defence University*, 13(4): 46-53. https://doi.org/10.53477/2284-9378-24-48

With the advance of the Red Army (later the Soviet Army, since 1946) into the territory of Bessarabia, as a result of the Uman-Botoşani operation and later the Iaşi-Chişinău operation, the Soviet authorities intensified the process of Sovietization and collectivization of the SSR. This process, which had begun as early as June 1940, was marked by forced collectivization, starvation, and mass deportations of the native population. The local Romanian population, as well as the non-Romanian one, showed reluctance towards the new authorities from the very first days of the occupation, expressing their disobedience through various forms of resistance. Among the multiple forms of anti-Soviet resistance during this period was the practice of desertion by young men conscripted into the Soviet Army, either by fleeing from military units or by evading military enlistment. The files of the party and Soviet bodies, as well as the military commissariats of the Moldavian SSR from 1944 to 1955, kept in the National Archives of the Republic of Moldova and the Archives of Social-Political Organizations of the Republic of Moldova, shed new light on this aspect of the history of resistance to the establishment the communist regime of that period. To the general notion of desertion, the Soviet military authorities attributed several meanings, among which the following were found: actual desertion from a military unit, evading enlistment in the ranks of the army and not appearing at the summons of the military commissariat, escaping from transport during the journey to the place of military service until upon taking the oath, not returning to the military unit from leave or medical treatment and others. Under the incidence of desertion also came pre-military young men compulsorily recruited for studies at vocational-technical schools (FZU) inside the USSR.

The massive mobilization of the population of the SSR began with the advance of Soviet troops on the territory of the country. The USSR was viewed by the Soviet military command as an important demographic source of replenishing the Red Army's losses suffered during the 1944 campaign on all fronts of operations. Between March and December 25, 1944, alone, hundreds of thousands of men were mobilized into the army, as follows:

- in the units of the Odesa Military Region – 115,504 people;
- in the units of the 1st and 2nd Ukrainian Fronts – 123,776 people;
- pre-military mobilized – 2,658 people;
- mobilized as a reserve of the Odesa Military Region – 21,343 people;
- in TOTAL – 263,281 people.

At the same time, 23,334 people were mobilized in the economy (AOSPRM, Fund 51, inventory 3, file 438, f. 4). But starting the mass mobilization of the population, the Soviet and military authorities collided with a new phenomenon for them, that of mass desertions of the mobilized population from military units or evasion from mobilization. From the beginning, this phenomenon received a pronounced anti-Soviet character. Thus, in June 1944, more than 300 newly mobilized soldiers from Soroca County, all Moldovans, led by Gumenâi Venedict (AOSPRM, Fund 51, inventory 3, file 431, f. 21). In June 1944, a group of deserters from the Red Army,

numbering 7 people, led by Ruga Ion, originally from the Rudi commune, armed with 2 rifles and an automatic pistol, operated in the forest from Otaci, and in the forest from Țeplenești, Bălți county, another group, headed by Chicu Grigorie, originally from that village (AOSPRM, Fund 51, inventory 3, file 431, f. 22). The most dangerous for the authorities was, however, an armed group of deserters, composed of 7 people, who were active in the commune of Șeptelici and whose goal was the armed struggle against the Soviet power (AOSPRM, Fund 51, inventory 3, file 431, f. 24).

The magnitude of the phenomenon was so great that it alarmed the military authorities who, in the informative note addressed on July 25, 1944, in the name of Nikita Salogor, First Secretary of the Communist Party of the Moldavian SSR, communicated that "among the Moldovans mobilized in the Army Red shows the tendency to desert from the army units aggravated by the anti-Soviet spirit" (AOSPRM, Fund 51, inventory 3, file 45, f. 48). Thus, only from the 35th Rifle Training Division, in July 1944, 32 trainees, all Moldovans, deserted from the districts recently "liberated" by the Red Army. It is symptomatic that the organizers of the fugitives, among whom N. Spinei stood out, as he was later sentenced to death by the Soviet judiciary, were in the past part of the Romanian army (AOSPRM, Fund 51, inventory 3, file 45, f. 48 verso). Alarmed by the growth of the phenomenon and to put an end to the growing tendency of Moldovans to flee from the ranks of the Red Army, a special commission was created within the central party and Soviet bodies, tasked with developing concrete measures to combat desertions, composed of 9 persons, as follows:

1. Comrade Proletarschi, head of the military section of the Bender (Tighina) county party committee;
2. Captain Mulita, deputy head of section 1, RSSM Military Commissariat;
3. Lieutenant-Major Ivliev, deputy head of section 1, fight against banditry, People's Commissariat of Internal Affairs (NKVD) of the RSSM;
4. Captain Cuceruc, deputy head of section 1, fight against banditry, People's Commissariat of Internal Affairs (NKVD) RSSM;
5. Comrade Haidalov, head of the military section of the Chisinau district party committee;
6. Lieutenant-major Corniuhin, deputy head of section 2, Strășeni district police station;
7. Comrade Minin, instructor of the Military Department CC PC(b) Moldova;
8. Captain Gologalov, secretary of the party organization of the Military Commissariat of the USSR;
9. Captain Kocetkov, head of section 2, fight against banditry, People's Commissariat of Internal Affairs (NKVD) RSSM (AOSPRM, Fund 51, inventory 3, file 431, f. 16).

Despite Bolshevik enthusiasm and efforts, the commission's work proved ineffective, ending in total failure. From month to month, the number of fugitives increased, also supported by the relatives who remained at home who urged them to flee in letters

sent to the army. Aware of the censorship of letters sent, even written in Romanian, many used code words or phrases and words written in the Gypsy (Roma) language, incomprehensible to Russians (AOSPRM, Fund 51, inventory 3, file 45, f. 1). Much more serious was the fact that deserters and those who evaded mobilization gathered in groups and began to wage an armed struggle against the Soviet power. Thus, in the Comratul Nou commune, on January 5, 1945, the father and son Slavovici killed the official F. Gherasimov, in charge of agricultural supplies, who intimidated the population with mass mobilizations in the army. His successor, who had just taken office, met the same fate, killed on January 11, 1945. On the same day, the secretary of the Chirsova village Soviet, V. Tafratov, was killed. Also active in Bugeac was a group of people who evaded military service, plotting the assassination of the presidents of the village soviets in Taraclia and Căinari (AOSPRM, Fund 51, inventory 3, file 89, f. 12). In the forest near the town of Olănești, a group composed of 85 people was hiding from the mobilization. In the first two months of 1945 alone, 3,226 deserters and people evading service in the Red Army and 980 deserters mobilized to work in the USSR industrial complex were detained in Bender (Tighina) county, a fact that could not jeopardize the announced plans regarding the mobilization of the population of the republic for war (AOSPRM, Fund 51, inventory 3, file 89, f. 13).

The analyzed documents demonstrate a surprising fact, for the current situation in the Republic of Moldova, but explainable, from a historical point of view, namely, the hostility of the population of Bugeac, mostly Gagauz and Bulgarian, towards the Soviet power and the Red Army and the sincere sympathies towards Romania. So, in March 1945, Baradja Maria, a Bulgarian citizen from the Taraclia commune, urged the locals to be a little more patient, because "in the spring of 1945 our liberators - Romanians will come to Bessarabia", and the resident of the Cazaclia town, Stefoglo Mihail, a Gagauz by nationality, urged the population not to cede their lands to collective farms, because "soon the Romanians will come to Bessarabia and ours must be helped [...] we must hide from the mobilization and meet the Romanian army". The resident of the Tătar Copceac commune, Anghelcev Tudor, a Gagauz by nationality, agreed and declared loudly that "it is at all costs necessary not to end up in the Red Army […] **because Bessarabia was and will be Romanian**". The president of the village Soviet from Cazaclia, Dobrova Xenia, deserves all the respect of the current generation, as, despite the position she held, not only openly claimed in front of the citizens that "life in the USSR is harmful to the peasants, and the communists are impostors, while the Romanians in the interwar period hung with respect for the Gagauz and there were no political reprisals", but she also warned the men from the date of mobilization so that they would have time to hide in the forests (AOSPRM, Fund 51, inventory 3, file 89, f. 20).

Despite the measures taken, the situation worsened every day. The extent of the phenomenon can be demonstrated by the number of deserters and evaders apprehended between April 1944 and April 1945, without taking into account those who were not caught, data presented in the following table:

TABLE 1

Number of deserters and evaders apprehended in April 1944 – April 1945
(AOSPRM, Fund 51, inventory 3, file 89, f. 19)

Judeţ	Number of evaders caught	Number of deserters caught
Chişinău	1 113	1 480
Soroca	1 894	4 091
Bălţi	2 082	3 478
Orhei	1 614	1 312
Bender (Tighina)	3 114	2 013
Cahul	2 315	1 905
Stânga Nistrului	810	901
TOTAL	12 942	15 180

The process continued with no less scope in the following years. In the years 1947-1948, 162 people who deserted from the army were registered (AOSPRM, Fund 51, inventory 7, file 60, f. 113). During the entire year of 1948 and four months of 1949, 240 cases of evasion from the Soviet Army, 208 cases of desertion and 30 people did not show up at the mobilization points were registered in the SRSM (AOSPRM, Fund 51, inventory 8, file 76, page 71). The processing of all existing documents allows us to find that, from 1946 to 1954, 228 cases of desertion from the ranks of the Soviet Army were reported. In fact, only 3 Russians, a Jew and a Buryat were certified among the deserters, the rest being Moldovans, including four people - Moldovans from the town. Chilia (Ukrainian SSR) denotes once again that the phenomenon of desertion had a pronounced national character of anti-Soviet resistance. The created situation can be presented in the following table:

TABLE 2

Number of deserters from the Soviet Army (by years)

Rayon	Year					
	1948-1949	1950	1951	1952	1953	1954
Bravicea						
Călăraşi				6	2	
Lipcani						1
Edineţ					3	
Drochia		1		3		
Străşeni						
Otaci						
Ocniţa					4	
Soroca						
Zguriţa						
Olăneşti						
Vulcăneşti						
Chipirceni						
Total - 84	**228**	**1**		**9**	**9**	**1**

The analysis of the table demonstrates that the maximum number of cases of desertion fell on the years 1948-1949, the most difficult years in the contemporary history of Moldova, when the process of forced collectivization took place, resulting in starvation and mass deportations of the population of the republic, which is still an additional argument that desertions from the Soviet Army, in the concrete conditions of the SSR in those years, became a form of anti-Soviet manifestation. The districts most affected by this phenomenon were Soroca, including Zgurița district, which was part of Soroca county and Bravicea district.
The absolute majority of deserters were caught by the militia bodies or by the military authorities and returned to their units, such as the case of soldiers Jardan Diomid, Moroșan Ștefan and Brașovean Nicolae, who, on June 11, 1950, fled from military unit no. 53609, but were caught on 15 June 1950 instead. Kamîșovka, Vladimir region (ANRM, Fund 2862, inventory 3, file 5, f. 2). A similar case took place on January 30, 1952, when Calin Ștefan, originally from the village of Buda, Călărași district, soldier of military unit no. 02151, ordered within Pereiaslavovka, Kaliningrad region, at 10 p.m., taking advantage of the lack of electricity, fled from the unit's disposal under the pretext of going to the old house. After a month of unsuccessful searches, he returned voluntarily, in February 1952, to the unit, not finding the possibility to leave the region (ANRM, Fund 2859, inventory 3, file 4, f. 8). The flight of the Greek soldier Dumitru, who left military unit no. 86716 on 06.01.1954 and was caught and returned to the unit on 07.01.1954 (ANRM, Fund 2859, inventory 3, file 10, f. 1) can also be mentioned.

There were also cases when the search lasted longer, the fugitives managed to hide from the Soviet authorities and, having travelled thousands of kilometres, arrived safely home. Thus, on the night of December 11 to 12, 1947, from the 492nd Independent Construction Battalion, located in the city of Novo-Fominsk, the soldiers Popescu Vasile and Coptari Timofei deserted. The following night, also from the same unit, the soldiers Negruță Ion, Gorman P. and Gulea I, all originally from the Zgurița district, did the same, going towards their homeland (ANRM, Fund 2875, inventory 3c, file 1, f. 7-8). Catching them was made difficult because the fugitives, arriving in their homeland, knew perfectly well all the places where they could hide, information that the local militia and military authorities, mostly coming from inside the USSR, did not have. The search, in the summer of 1948, for the deserters Guțu Vasile and Ceban Gheorghe, who avoided all the raids and ambushes organized by the military bodies in collaboration with the local militia, was also unsuccessful, as they managed to hide in the forest and the fields of corn (ANRM, Fund 2875, inventory 3c, file 3, f. 25). Lucky also turned out to be the soldier of the 7th guard company, South Operative Group (Romania), Șandra Vasile, a native of Ciuciuleni commune, Strășeni district, who deserted from the unit in December 1946, searched until October 1949, without being found (ANRM, Fund 2873, inventory 4, file 8, f. 5). We can only assume that he remained in Romania, being hidden by the population.

Among the cases of desertion, there were also absolutely exceptional examples. If the success of V. Șandra's escape from the military unit can be explained by the possible help given to this Moldovan by the population of Romania, among which he could easily hide his Soviet citizenship, then the escape carried out by the soldier Cozubenco Ion, seems as if taken from a novel of fiction. On March 27, 1950, Ion Cozubenco, a soldier in the 459th Independent Airfield Technical Security Battalion within the Soviet military occupation group in Germany, and a native of Palanca, Călărași district, took advantage of the fact that, at that time, the Soviet occupation zone in Germany was still completely separated from the Western occupation zones. He left his unit and fled to the American occupation zone (ANRM, Fund 2859, inventory 3, file 4, f. 14), thus becoming inaccessible to Soviet justice.

The anti-Soviet nature of the desertion phenomenon can be easily demonstrated by the existence of armed groups formed by deserters who were active in the territory of the SSR. A representative example is the case of Ștefan Ion Bătrîncea, who, after being conscripted into the Soviet Army by the Călărași Military Commissariat, fled from the recruitment assembly point on December 11, 1950. He went on to form an armed group that, over two years, terrorized the local Soviet authorities. Only after special security forces were involved in his capture, on July 14, 1952, was he arrested and brought to justice (ANRM, Fund 2859, inventory 3, file 4, f. 4). A group of deserters, composed of six people, was also active in the summer of 1948 in the town of Sudarca, Otaci district (ANRM, Fund 2891, inventory 2, file 2, f. 70). An illegal anti-Soviet group was also formed in the summer of 1949 in the village of Recea, Strășeni district, which was active within that district. This group, in 1949, killed the president of the village Soviet from Pănășeni commune, and in 1950 seriously injured the secretary of the UTCL (Komsomol) organization from Zubrești. In the summer of 1950, the members of the group were arrested by the security authorities (ANRM, Fund 2879, inventory 3, file 4, f. 4).

In conclusion, we can state that, during the period 1944-1954, the desertions of the autochthonous population from the Moldavian SSR had a massive and clear anti-Soviet character, becoming a form of the struggle of the Moldavians against the Soviet occupation. Over time, thanks to the retaliatory measures, but also the "taming" of the Soviet regime during the Khrushchevist "thaw", this phenomenon disappeared as a manifestation of the anti-Soviet trend.

References

Archive of Social-political Organizations of the Republic of Moldova (AOSPRM), Fund 51, inventory 3, file 45.

__. Fund 51, inventory 3, file 89.

__. Fund 51, inventory 3, file 431.

__. Fund 51, inventory 3, file 438.

__. Fund 51, inventory 7, file 60.

__. Fund 51, inventory 8, file 76.

National Archive of the Republic of Moldova (ANRM), Fund 2862, inventory 3, file 5.

__. Fund 2859, inventory 3, file 4.

__. Fund 2859, inventory 3, file 10.

__. Fund 2873, inventory 4, file 8.

__. Fund 2875, inventory 3c, file 1.

__. Fund 2875, inventory 3c, file 3.

__. Fund 2891, inventory 2, file 2.

__. Fund 2879, inventory 3, file 4.

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

Contributions to the elucidation of a controversial episode. The Ciulei Case. (2)

Col. Liviu CORCIU, Ph.D.*
*The Romanian National Military Archives
e-mail: liviu.corciu@yahoo.com

Abstract

Based on previous documentation, not necessarily the subject of this article, we can state that the administration of military justice in the War of the Integration was not a perfect process, among the most important criticisms being the judicial errors recorded, on the one hand, and the interference of commanders in the act of justice, on the other. The fact that the members of court martial panels were appointed by the commanders of the major units with which they operated, from the divisional level upwards, was a procedure that naturally facilitated the existence of subordination relationships, with a direct effect on the administration of justice. Another explanation for the low quality of justice is the lack of specialized training of the members of the councils of war and courts-martial, the training of the officers called upon to carry out military justice being encumbered by the educational system of the time. It is in this context that the trial of Second Lieutenant Constantin Ciulei should also be analyzed, which thus takes on new meanings and significance. The disciplinary situation of the troops called for an exemplary punishment, which was swiftly carried out and significantly impressed the audience, and the fact that Ciulei was an officer was an asset that ensured the notoriety of the event.

Keywords:
court-martial; summary execution; deserter; military justice; miscarriage of justice.

Article info
Received: 26 June 2024; Revised: 22 August 2024; Accepted: 7 November 2024; Available online: 17 January 2025

Citation: Corciu, L. 2024. "Contributions to the elucidation of a controversial episode. The Ciulei Case. (2)". *Bulletin of "Carol I" National Defence University*, 13(4): 54-76. https://doi.org/10.53477/2284-9378-24-49

Validation

As we promised at the beginning of this article, we will address, one by one, all the hypotheses put forward in the two articles in *Magazin Istoric* and *Avântul*, with arguments drawn from primary sources. Thus, we do not consider as valid the first hypothesis, according to which Ciulei's being put on trial would have been done to confuse the suspicions of the commander of the 2nd Army, since putting Ciulei on trial was Sturdza's second option; the first one, as we have already presented, was to shoot him on the spot, to set an example to the demoralized troops. A summary execution, which did not involve sending him before a full court.

Moreover, it is obvious that those questionable retreats of the 7th Mixed Brigade, which had drawn the attention of General Averescu, (Monkevitz and Vinogradski 2019, 33) involved the defensive deployment of the entire brigade and required a higher level of decision, and could not be attributed to a second lieutenant (Monkevitz and Vinogradski 2019, 33), etc.
Neither do we consider valid the second hypothesis, according to which Sturdza, suspected of treason, *would have put everything on Lieutenant Ciulei, whom he blamed for having withdrawn from the position, without orders, together with his subunit*.

Firstly, on December 26, 1916, Sturdza was not suspected of treason. His previous decisions to withdraw, unjustified in General Averescu's opinion, had caused his displeasure, but from here to the suspicion of treason was a long way off.
General Averescu did not understand Sturdza's repeated retreats, probably fearing the proximity of the sector occupied by the 7th Mixed Brigade to the Russian troops. The decisions in Sturdza's sector could have negatively influenced the relationship with the Russian allies, although, paradoxically, they seem to have had an excellent impression of the 2nd Army troops. In his memoirs, the Russian General Nikolai A. Monkevitz wrote about *"the regiments of General Averescu's heroic army",* mentioning that he had the opportunity to meet them several times and that he was amazed by *their "iron discipline, (...) impeccable organization",* etc.
Secondly, it was not the retreat on *Momâia* that General Averescu referred to in his memoirs, but the retreat at *Soveja*, which had taken place two days earlier, on December 24. And, thirdly, it was not Ciulei, but Mărculescu, who had been accused of the hasty escape from *Momâia*.

In our opinion, the third hypothesis, according to which *Ciulei was* ***suddenly*** *accused* (s.n.) *of treason by Colonel Sturdza,* is not valid either. This *suddenness* induces the idea that Ciulei was, in relation to Sturdza, *the scapegoat* or the guilty one, a momentary solution, a sudden solution for what happened on *Momâia*. The accusation of treason brought against Second Lieutenant Ciulei was not an untimely act, in the sense that it did not come *suddenly*. Initially, Sturdza wanted to set an extreme example to the troops by executing Captain Marculescu and Second

Lieutenant Ciulei, both officers, both commanders of sub-units, in front of their own subordinates, without trial. The failure of this plan led, in fact, to the initiation of treason charges against both of them. Sturdza's only option was to refer the matter to the royal commissioner of the 1st Infantry Division since the accusations had been made public and the attempt to execute the two officers had failed.

Why did Sturdza refer the matter to the 1st Infantry Division? On the one hand, this echelon had the competence given by the Code of Military Justice to deal with the case, and on the other hand, the court-martial, as a military court, could be organized only from the division echelon upwards, by order of the commander of the respective structure. Except the officers, who were, as a rule, tried by the court martial constituted at army level.
Sturdza could not organize his own court-martial at the 7th Mixed Brigade, and besides, neither Captain Marculescu nor Second Lieutenant Ciulei belonged organically to the 7th Mixed Brigade but had been seconded to this large unit.

The entire staging of this *summary execution* was, in our opinion, a spontaneous gesture on Sturdza's part, intended to impress the audience and to set an example for the soldiers, who should have been aware of the possible consequences they would have faced if they had risked a similar gesture.
We believe that Sturdza's intention to punish Mărculescu and Ciulei was not premeditated, and the arguments supporting this claim invalidate, in our opinion, the hypothesis of Prof. Nicolau's article. The assertion is based on the fact that Sturdza witnessed the performance of the two men on *Momâia, a* fact confirmed by the testimonies of Major Constantinescu and Lieutenant Marinescu. Moreover, at the time of execution, neither Mărculescu nor Ciulei were tied up, as required by the firing squad procedure, nor even disarmed.

Nor do we consider as valid the fourth hypothesis, according to which *Second Lieutenant Ciulei was convicted because the court-martial was intimidated by the situation of the accuser*. The expression *"situation of the accuser"*, used by the press of the time, probably referred to Sturdza's position in the army and society. The claim about Sturdza's influence in society is questionable. Even in his memoirs, he mentions that he felt threatened by the Brătianu family, and his and his family's political orientation was clearly pro-German and deeply anti-Russian. We also have reservations about Sturdza's alleged influence in the army, especially among the officers of the 2nd Army, but in particular on the members of the 2nd Army's court-martial court-martial panel, whom we have managed to identify and will present later.
As for the influence Sturdza may have had on General Alexandru Averescu, from the latter's memoirs it emerges that Sturdza did not enjoy a privileged position, but on the contrary, Averescu did not even want him in his subordination, considering him a vain, *"more a nuisance than a help"*. (Averescu 1992, 104).
The fact that Sturdza was changed from the command of the 15th Infantry Division, subordinated to the 2nd Army, where he had been initially appointed, to the

command of the 10th Infantry Division, subordinated to the 1st Army, which was being replenished in northern Moldavia, could be interpreted as a clue in support of this claim. This is why we subscribe to the opinion (Otu and Georgescu 2011, 137) that at the time of the trial of Second Lieutenant Ciulei, Sturdza had no way to intimidate the trial panel, since his disappearance had already been reported, in unspecified circumstances, since the night of January 23/24, 1917.

The fifth hypothesis, according to which *Ciulei was executed and Sturdza deserted,* is misrepresented in terms of the chronology of events. As we have already said, Sturdza had already deserted on the night of January 23/24 and was initially considered missing. The corpse of his ordinance, the footprints in the snow leading to the enemy lines, and the personal luggage in which his diary was found, fueled suspicions of a possible act of treason. However, the confirmation of treason came after the capture of Crăiniceanu, on January 28, at noon, and officially materialized in the afternoon of the same day, after he confessed to the meeting with Sturdza and the manifests instigating treason were found.

Ciulei was tried on January 26, sentenced to death, and executed on the morning of January 28, at 10.00 a.m., at the firing range in Bacău, where the 2nd Army command post was located, whose court-martial had tried him. Thus, at the time when Ciulei was dying in front of the firing squad, Crăiniceanu had not yet been caught, and Sturdza's desertion was still at the stage of disappearance under unsolved circumstances.

The sixth hypothesis, that *Ciulei was innocent, but suspected Sturdza's links with the enemy,* is also groundless. Sturdza did not intend to shoot Ciulei because he suspected his links with the enemy. This theory emerged later, perhaps promoted by Marculescu himself, as we shall see from his memoirs, and was certainly fueled by the theories woven after Sturdza's defection.
Ciulei could not have suspected Sturdza's connections with the enemy, first, because he had joined the 7th Mixed Brigade only a few days before, and like most of the newcomers, officers and troops alike, did not even know him.

Secondly, Ciulei was at a much lower level of the military hierarchy, not even part of the brigade staff. He was a junior officer, according to the denomination of the time, whose place was in the middle of his subunit, which would not have allowed him to be around Sturdza to see how, and above all, what he thought.
It is even very probable that the position of commander of the battalion reserve was entrusted to Ciulei by his former comrade and hospital colleague, Captain Mărculescu, precisely because this would have facilitated a cantonment near him, knowing that, as a rule, the battalion reserve is usually located near the command point, and its commander is at the battalion commander's disposal.
Neither the last hypothesis, according to which *Sturdza realized that he could have unmasked and dismissed Ciulei, influencing the court-martial towards a decision to*

sentence him to death, can be validated, in our opinion, based on the arguments that we will present below.

We first state that this last hypothesis tested is, in fact, a combination of two of the hypotheses argued above. The first one induces the idea of Sturdza's premeditation of the act of desertion, or at least of its existence, even in latent form, since December 26, 1916, when the episode of the failed execution of Mărculescu and Ciulei took place. The second one suggests that Sturdza's decision to make an example of the two, but especially of Ciulei, was motivated by the fear of not being unmasked, and thus influenced the court-martial to sentence the latter to death. The fact that, in our opinion, Sturdza could not have influenced the court-martial of the 2nd Army is a statement that we have argued above, and that is also shared in the book by professors Petre Otu and Maria Georgescu.

As for Sturdza's decision to go over to the enemy, we cannot assess the exact moment, but it was certainly after December 26, 1916, when the *Momâia* episode took place. We believe that regardless of his political beliefs and the notoriety of his pro-German attitude, the crystallization of the idea of going over to the enemy camp took place after he effectively surrendered command of the 7th Mixed Brigade, and this event took place on January 4, 1917.

The memoirs (Scărișoreanu 1934, 174) of General Romulus Scărișoreanu show that as early as December 26, 1916, Sturdza would have been appointed to command the 15th Infantry Division, which is why Scărișoreanu, then a colonel, would have been called to take command of the 7th Mixed Brigade. But his immediate superior at the time, General Eremia Grigorescu, knew nothing about this appointment, and Sturdza's appointment never materialized. The situation validates (Averescu 1992, 104) what was recorded, on the same date, in the memoirs of General Alexandru Averescu, who confirmed Sturdza's appointment as division commander, but also clearly stated that he did not want him as a subordinate and that he hoped *"to get rid of him"* (Averescu 1992, 104).

In fact, some sources (Kapri 1926, 14) indicate a close connection between the moment when Sturdza decided to switch to the enemy camp and the change of the decision of the Great General Headquarters which, although it had initially appointed him to the position vacated by the promotion of General Eremia Grigorescu, in command of the 15th Infantry Division, subordinated to the 2nd Army, changed its decision by appointing him to command the 10th Infantry Division, which was in the depth of its own device, in the north of Moldavia.
Probably feeling rejected by his hierarchical superiors, which questioned his performance so far in command of the brigade, his refusal to be entrusted with the command of a renowned division, in contact with the enemy, and his being sent in the proximity of *the "real enemy"* (Kapri 1926, 8), as he used to say, were decisive in Sturdza's *"wretched decision* " (Kapri 1926, 6).

What is more, the decoration that King Ferdinand gave him personally, following the meeting a few days earlier, was no more than a pale consolation. Or the candy that should have sweetened the bitterness of frustration. According to this logic, at the time of December 26, 1916, the hypothesis that Sturdza had given in to *the fear of not being unmasked* cannot be considered as a motive for his actions against Mărculescu and Ciulei.

Court

However, the question still remains: *Why the rush to try and convict Ciulei?*
In an attempt to answer this natural question (Otu and Georgescu 2011, 137), as to the reason for the haste with which this case was tried, we have found a possible explanation in the memoirs of Lieutenant-Colonel Mihai I. Buttescu. The former commander of the "Regina Elisabeta" 2nd Hunting Regiment considered General Gheorghe Mărdărescu, Chief of Staff of the 2nd Army, guilty of having *appointed* General Gheorghe Mărdărescu, the chief of staff of the 2nd Army, as president of the court-martial (the court-martial was appointed by order of the commander, s. n.) (Buttescu 2012, 314) a former subordinate, an obedient character, categorized by the author as *an instance of nepotism*, in the person of Colonel Alexandru Alexiu, "*who sentenced to death for reasons not sufficiently investigated (the case of Lieutenant Ciulei) and* ***executions were daily*** (s.n.)*".*

From the verifications carried out in the documentation of the present work, it emerged that this assertion is confirmed, both in terms of the existence of the previous subordinate relationship of Colonel Alexandru Alexiu to General Gheorghe Mărdărescu and in terms of Colonel Alexandru Alexiu's fulfillment of the function of President of the 2nd Army's Court Martial.
Thus, in 1915, Colonel Alexandru Alexiu served as commander of the *Infantry Shooting School* at Mihai Bravu, General Gheorghe Mărdărescu being his immediate boss, then *Technical Inspector of the Infantry*. Moreover, in the 1918 *report card of* the first one, General Gheorghe Mărdărescu stated: *"I know his* (Colonel Alexandru Alexiu's) *activity in the campaign* (Colonel Alexandru Alexiu, s.n.) *as he was under my orders almost all the time* (Romanian National Military Archives File no.6, f.30)*".*
As for the confirmation of the second assertion, we have identified *"Address no. 16004"* (Romanian National Military Archives, file no.1691, f. 9-10) dated January 23, 1917, by which the court martial of the 2nd Army forwarded to the Military Justice Service of the General Headquarters a table with the nominal composition of the court-martial that functioned in the subordinate divisions.

In the first position of the table attached to this address is Colonel Alexandru Alexiu, President of the court martial of the 2nd Army. Next to him, the court panel, which may also have convicted Ciulei, was composed of Major Constantin Tănăsescu, Major Nicolae Opran, Captain Ion Glogoveanu, and Captain Titus

Carapancea. We approach the composition of the trial panel as a possibility and not as a certainty since the panel could have been made up of the president and three permanent members, depending on the rank of the accused and the dispositions of the appointing commander. The 2nd Army also had Lieutenant Colonel Gheorghe Pangrati as Royal Commissioner, and Major Mihail Protopopescu as substitute Royal Commissioner. It is therefore confirmed that, at the time of the trial of Second Lieutenant Constantin Ciulei, Colonel Alexandru Alexiu, commander of the 2nd Army Training Center (Romanian National Military Archives, file no.6, f. 27), was acting as president of the trial panel.
Moreover, we also identified (Romanian National Military Archives file no. 37, f. 694) an order signed by Colonel Alexandru Alexiu, in his capacity as president of the trial panel of the 2nd Army court-martial, by which Captain Mărculescu, who had not been caught until that moment, was sent to trial at that court-martial as a deserter, together with Second Lieutenant Zodilă, who was mentioned above, and who was known to have willingly joined the enemy, also on the same day.

As for the claim regarding the rhythmicity of executions, the information is partially confirmed by the summary entitled *"Monograph of Military Justice during our War"* (Romanian National Military Archives file no. 924, f. 1), more specifically, by what is recorded in the *"Statistical table of the number of death sentences by rank and deeds of those sentenced to death by military criminal courts during the war 1916-1918 executed until June 1, 1918"* (Romanian National Military Archives, file no. 924, f. 14), where the court martial of the 2nd Army is credited with 49 executions, by far the most of all court-martial and war councils during the period analyzed.
However, we are not certain that all these executions were due to the zeal of Colonel Alexandru Alexiu, as Lieutenant-Colonel Mihai I. Buttescu claims, which gives us the right to have reservations about his claims.

Of course, there are also other opinions regarding the speed with which the court-martial of the 2nd Army tried the Ciulei case, *"an unfortunate chain of events"* (Otu and Georgescu 2011, 137), which was due to the general context in which the Romanian army was operating, and the need to restore order and discipline, even by urgently repressing serious acts. We will analyze this opinion below.

Concerns

For a better understanding of the events in this case, we have also analyzed the correspondence between the General Headquarters and the 2nd Army on this subject. Headquarters was concerned about the situation in the sector of the 7th Mixed Brigade, whose initial report on the events of December 26, 1916, it considered *"very confused"* (Romanian National Military Archives, file no. 160, f. 23), and requested, by *"Telegram No. 4478"* of December 31 (Romanian National Military Archives, file no. 160, f. 23), 1916/January 13, 1917, clarifications from the 2nd Army, its higher echelon.

The situation that the General Headquarters considered *confusing* was the one reported telegraphically by the 2nd Army, which in turn relayed to the General Headquarters *"Report No. 2709"* (Romanian National Military Archives, file no. 160, f. 21) of December 28, 1916 by Colonel Alexandru Sturdza. In this report, Sturdza accused the officers of the battalion commanded by Mărculescu, and Mărculescu in particular, of the inadequate condition of the troops under his command and, in particular, of the event of December 26, 1916, on *Momâia*.
Ever since he took over the 7th Mixed Brigade, Sturdza claimed that Marculescu had shown *complete inertia in* the exercise of his command. He was not aware of the number of troops he had under his command, and for several days in a row, he had reported a strength of 500 soldiers, while in reality he had 700 soldiers under his command, whom he had not organized until that date, and 400 more were about to report.
As for the event of December 26, 1916, on *Momâia*, Mărculescu was accused of leaving the men to their own formations, *"unhinged, unoriented and unsupervised, and the officers were reporting fantastic* (untrue, s.n.) *news from* [to] *the enemy uncontrolled by the captain*" (Romanian National Military Archives, file no. 160, f. 21).

From this report, we also learn that Sturdza accused Mărculescu of the fact that every day in the sector under his responsibility there was panic, in which the officers took part, and that they were understood to have agreed to go over to the enemy. The most serious accusation, however, was that, on December 26, 1916, when the German attack occurred and the 3rd Company was broken up, not only was Mărculescu 1 km behind his battalion's positions, *at the roast*, according to Sturdza, but he also fled, leaving it to the latter to re-establish the position. He later reported that he would *hold his position* on the road, as he had been deserted by the soldiers.
"This commander was, in my opinion, the main culprit for the betrayal of the officers and the troop" (Romanian National Military Archives, file no. 160, f. 21), Sturdza concluded and concluded the report by summarizing the act of Marculescu's execution, which I have already described above.

This report was transmitted to the General Headquarters by the 2nd Army with *"Telegram No. 2881"* of December 29, 1916-January 11, 1917, and naturally aroused the concern and puzzlement of the higher echelons. Concern, on the one hand, because of the serious accusations of *treason* and *flight from the enemy* against an entire battalion, headed by officers and its commander, and puzzlement, on the other hand, because of the ambiguous account of the execution of an officer.
By *"Telegram no. 4478"* (Romanian National Military Archives, file no. 160, f. 22) of December 31, 1916/January 13, 1917, signed by General Constantin Prezan, transmitted through the telegraph machine "*Hughes*", the General Headquarters asked the 2nd Army to ask Sturdza to report *clearly and precisely* what measures he had taken against the officers he accused of having transmitted false information about the enemy, what measures he took the first time when panic broke out in the sector of his units when exactly he found that the officers were agreeing with the soldiers *to go over to the enemy*, to nominate the officers accused of treason, etc.

From the contents of the telegram, but especially from the tone and attitude of the General Headquarters, it is clear that the good faith of Colonel Alexandru Sturdza was not questioned at that time. On the contrary, the higher echelons even inquired about the measures taken against the commander of the platoon in charge of the failed execution of the two officers, who, in the opinion of the General Staff, should have been immediately sent to the 2nd Army's council of war and the result of the sentence should have been communicated to the higher echelons as soon as possible. In *Telegram no. 4478*, General Gheorghe Mărdărescu, Chief of Staff of the 2nd Army, sent a reply to the General Headquarters in the form of "*Telegram no. 2942* from January 13, 1917, which is deciphered (Romanian National Military Archives file no. 160, f. 09-10) in the same fonds. It presents the official version of the events on *Momâia*, dated December 26, 1916, stating that Sturdza had ordered Marculescu, during a visit to his sector only the day before, *"to immediately execute the panic provocateurs"* (Romanian National Military Archives, file no. 160, f. 09v).

Another element of interest for our investigation is the fact that General Mărdărescu stated in *Telegram no. 2942* that Sturdza moved on December 26, in the sector of Mărculescu's battalion on *Momâia, "on purpose to set an example"* (Romanian National Military Archives, file no. 160, f. 09v). The German attack and the surrender of the 3rd Company took place while Sturdza was at the very command point of Mărculescu's battalion, followed by the entire battalion, including its commander, fleeing from their positions.

The position was re-established, the 2nd Army telegram states, by Sturdza and Lieutenant Marinescu who accompanied him, *"with men hastily assembled and the fire of his* (Sturdza's, n.n.) *revolver"* (Romanian National Military Archives, file no. 160, f. 09v) . Once the situation on *Momâia* was re-established, the fugitives were assembled in the quay, "*with the officers in front of the front"* (Romanian National Military Archives, file no. 160, f. 09), Colonel Sturdza, the telegram stated, would have proceeded to a summary search, after which he would have announced the verdict: *the death sentence of* Captain Stelian Marculescu and Second Lieutenant Constantin Ciulei, who, according to what the Chief of Staff of the 2nd Army reported, were *executed* on the spot.

Here we would like to point out that, contrary to what is recorded in the source quoted in *Magazin Istoric,* in which Colonel Alexandru Sturdza allegedly ordered "*some soldiers to shoot at them and he himself fired a few rifle shots*" (Romanian National Military Archives, file no. 160, f. 09), the telegram of General Gheorghe Mărdărescu officially records the version in which Sturdza himself shot the two officers: *"It was not the time, nor was it opportune to have formed a firing squad; the brigade commander himself fired"* (Romanian National Military Archives, file no. 160, f. 10).
The darkness certainly contributed greatly to the missed execution, but Sturdza rather shot only Mărculescu, not Ciulei. Probably when he saw that Sturdza was about to kill him, Ciulei jumped into the nearby river and fled through the woods,

being caught later, while Captain Stelian Mărculescu, "*wounded in the neck and left arm*" (Nicolau 1974, 87), fell motionless in the snow.
According to the 2nd Army report, the latter, presumed dead, then jumped up at the approach of the medic and stretcher bearers, *"threatening them with a revolver"* (Romanian National Military Archives, file no. 160, f. 10) and fled into the woods.

The trial

Returning to the moment when the fugitives of the battalion commanded by Mărculescu were gathered on the *Varnița-Răcoasa* road, we deduce from the reports that Sturdza had arrived there after having re-established his position on *Momâia*, together with Lieutenant Marinescu of the 10th Călărași Regiment and the fugitives they had managed to turn back under the threat of revolvers. At about the same time, Polihroniade arrived, having rounded up the fugitives, including Ciulei from *Varnița*.
Determined to set a drastic example, in fact, the main reason why he had come to *Momâia*, Sturdza gathered the fugitives of the battalion in the quay, *"with the officers in front of the front"* (Romanian National Military Archives, file no. 160, f. 10), as the 2nd Army report shows, after which two other stages also mentioned in the report followed: their *summary trial*, ending up with their *execution*.

We did not find in our documentation how exactly the execution took place, given that the 2nd Army *Telegram no. 2942* shows that the officers were in the carriage, in front of the other fugitives. We later found out from Polihroniade's reports that all the officers in the battalion were considered responsible, and ten of them, including Mărculescu and Ciulei, were even nominated.
It is possible that after the guilt of Mărculescu, in his capacity as commander, and Ciulei, the latter, as I have said, as commander of the reserve that should have executed the counterattack, the others were put in formation and Sturdza fired at the former. The 2nd Army report says that Marculescu fell motionless in the snow, and was considered dead, after which the troop uncovered and a prayer was said. There followed an "*admonitory*" (Romanian National Military Archives, file no. 160, f. 10) speech by Sturdza, to make a good example of the spectacle the people had witnessed, after which the troops left for their positions under Major Constantinescu.

It seems that Sturdza would have ordered that the body of the "executed" should be brought to him, which is why the battalion doctor and the stretcher-bearers approached the place where he lay motionless in the snow, and Marculescu *"jumped up threatening with his revolver and fled into the woods"* (Romanian National Military Archives, file no. 160, f. 10v).

The telegram ends with an assurance to the higher echelons that order had been restored, proof that the troop had successfully held their positions the next day, repelling a German attack. However, the higher echelon was assured, as a safety

measure, a machine gun was in position behind the front, aimed (Romanian National Military Archives, file no. 160, f. 10v) at this troop's position, in case the example just set might not be enough.

Queries

It appears from *Telegram no. 2942* that Sturdza had had no interaction with Ciulei up to the time of his summary execution. It is clear to us that Polihroniade knew Ciulei, but there is no indication that Sturdza knew him. *And yet, why did Sturdza want to kill Ciulei,* as one of the hypotheses goes?
First of all, Sturdza had come to *Momâia* on December 26, because the position was a very important point on the Romanian-Russian front, and he understood the vulnerability of this sector for which he was implicitly responsible. Only two days before, on December 24, Sturdza's brigade had withdrawn *"without apparent cause, precipitately and without warning me in time"* (Averescu 1992, 102), as General Averescu wrote in his memoirs, turning Christmas Eve into the worst day of his life. At the same time, Sturdza realized that this important sector was occupied by a *close* battalion, to whose previous training he had not been able to contribute, commanded by an officer he knew he could not count on.

General Scărișoreanu also mentions the fighting cohesion and discipline of such a unit in his memoirs, when he recounts the decision of the 7th Infantry Division, to which he was subordinate, to exchange a company from the 3rd Hunters Regiment, which had initially been given to him in support, for a company from a supplementary regiment, made up of the remnants of other units, which had been found useless behind the 2nd Army: *"(. ...) in addition to its lack of homogeneity, it also presented itself in a disheveled appearance that did not inspire any confidence, which is why I never send it to the 1st line, and keep it only in reserve"* (Scărișoreanu 1934, 193).
Secondly, Sturdza had come on *purpose* to set an example because in the battalion's sector, every day, the panic was occurring, and what was even worse, these panic manifestations were attended by officers.

Panic

In our opinion, the rapidity with which Ciulei was tried, sentenced, and executed has nothing to do with Sturdza, but with a much more dangerous phenomenon. It was *panic*, a phenomenon that frequently occurred among demoralized and tired troops, who fled from their positions or, worse, deserted voluntarily to the enemy. Until January 19, 1917, the General Headquarters had not been informed of this phenomenon through the operational communications of the 2nd Army but had learned about it from enemy communications.

More precisely, the moment they realized that the Germans were not lying in their communiqués about the number of those captured, but that the figures were even higher, and that everything had happened in such a short time and on such a small front sector, they realized that they had to take drastic measures.

Panic, individual or collective fear, is taken to extremes, and manifests itself on the battlefield through *non-combat*, refusal to fight, throwing down weapons and equipment, fleeing from position or voluntary surrender, or a combination of the above. In this kind of situation, fear persists, it does not go away easily, but it can be controlled. The level of this control is a projection of troop morale and one of the key concerns of the officers of that troop. They should have been firm, an example of moral stability and courage, and should have constantly encouraged their subordinates.

Sturdza had foreseen the possibility of this phenomenon in his brigade's units since the beginning of the war. On September 20, 1916, he issued the *"Circular on Preventing Panic Panics"* (Romanian National Military Archives, file no. 21, f. 176) in which he described panic to his subordinates as a symptomatic phenomenon that had occurred in past and present conflicts in our and other armies, and he set specific tasks for commanders at all levels of command.
The main feature of this phenomenon was considered to be *contagion*, followed by *rapid transmission* among the troops, originating from rumors, noises, unexpected movements, shouts or alarm signals, etc.
Sturdza assured his subordinates that *"Panic does not exist in any environment, a well-trained troop (...) and which knows its commanders well, a troop where (...) brotherly solidarity reigns (...) between officers of all ranks and soldiers (...) does not become alarmed as easily as another, where the chiefs live apart from their inferiors, where trust does not exist and authority is imposed only through disciplinary power"* (Romanian National Military Archives, file no. 21, f. 176).

In order to avoid such harmful manifestations, Sturdza ordered the company, squadron, and battery commanders to talk to the men every day, to *orient the troops* by a simple, sincere, and confident exposition of the situation, and above all to forbid, and even punish, the spreading of rumors.
This circular order concluded that, by their attitude, officers could greatly influence the troops, and could keep it from panic, through the power of moral authority: *"The problem to be solved* (sic!), he added, *is a matter of education, organization, and leadership and in the first line* (first of all, s.n.) *of personality and character"* (Romanian National Military Archives, file no. 21, f. 177).
We know from the communication of the 2nd Army that on December 25, so only a day before, Sturdza had given Mărculescu the order to immediately execute those of his subordinates who were spreading panic rumors. This order was a *blank check*, and Sturdza probably had no warning of any such measure. At the time of reading this article, and knowing Mărculescu through the prism of the characterizations

of his hierarchical chiefs, it is clear to us that Sturdza's expectations of a man of Mărculescu's temperament were totally unrealistic. Lacking energy, melancholic, sickly, complexed by a nervous tic and a clumsy, peevish expression, Mărculescu would have been impossible to impose himself on his subordinates, as we have said earlier, let alone shoot them.
As for Ciulei, although in Sturdza's eyes, he shared the guilt jointly and severally with the entire battalion's officers, this was not the aggravating circumstance of his status, but in our opinion, the position held in Mărculescu's battalion, that of battalion reserve commander.

The explanation could be, in our opinion, linked to the very role of the battalion reserve which, as a rule, intervenes in the battle by executing the counterattack when the battalion's defensive line is breached. It would therefore have been Ciulei's task to enter the battle and counterattack with the two platoons subordinated to him when the Germans occupied the battalion's positions on *Momâia*. However, Lieutenant Marinescu's testimony shows that at the first contact with the enemy, the second lieutenant in command of the battalion reserve fled with the platoons of his subordinates. Also, Polihroniade's report shows that he would have found Ciulei in *Varnița*, far behind the front, with the two platoons he commanded. This argumentative construction invalidates, once again, the hypothesis that Sturdza premeditatedly wanted to kill Ciulei because he had guessed his intentions to switch to the enemy and that later, for the same reason, he would have court-martialed him.

Sturdza knew Mărculescu before the event on *Momâia*, as he himself said, from *Câmpuri*, when he personally went to see him because he reported considerably lower numbers than in reality. However, there is no evidence to suggest that Sturdza had previously known Ciulei. Sturdza knew Mărculescu, but he did not appreciate him at all, considering him absolutely inert in the exercise of his command and lacking empathy with the situation of his subordinates, about whom he did not know, as I said, not even approximately, how many there were.

Although at first glance this accusation might not seem very serious, in the context of the resubordination of his battalion to the 7th Mixed Brigade, Mărculescu should have known at all times exactly how many soldiers he had under his command. Anyone who has served in the army or has any connection whatsoever with such a system understands that according to its manpower, a sub-unit is assigned to the food rule, its equipment, armament, and ammunition are distributed and its missions are determined.

If it had been true that Mărculescu had reported a strength of 500 soldiers, when the real strength was 700 men, it would have meant, in terms of food alone, 200 fewer meals a day for his subordinates. The result of this administrative "oversight" would not have been in any way able to raise the morale of the troops, given the living conditions on the 2nd Army front, which I have presented.

Press releases

From December 31, 1916/January 13, 1917, when General Gheorghe Mărdărescu informed the General Headquarters about the events of December 26 on *Momâia*, until January 20, 1917, I have not found anything of note in the military archives on this subject. On December 28, as I have mentioned, Ciulei had been arrested in the house of a householder in *Verdea,* and court-martialed, and his case was following its hierarchical course.
In the meantime, Sturdza had handed over command of the 7th Mixed Brigade on January 4, 1917, and was appointed to command the 10th Infantry Division, an appointment which, as I have argued previously, seems to have led him to decide to betray.

Something did happen in the present case, however, between December 31, 1916, and January 20, 1917, something that may also explain the haste with which Second Lieutenant Ciulei was put on trial, convicted, and executed. A reason other than Sturdza's influence on the 2nd Army court-martial panel, is a hypothesis on which we have ruled, presenting our arguments above.
Thus, it is quite possible that the General Staff, not Sturdza, wanted to set an example in order to stop the phenomenon of desertion, and Ciulei was considered to be the right example. He was already in the custody of the military authorities after he had tried to flee, his case was already under investigation, and the accusations against him were related to a subject in which the Great General Headquarters showed an undisguised interest.

Otherwise, it would not explain why since December 31, 1916, when General Mărdărescu had fully informed the General Headquarters about what happened on *Momâia*, the reaction of the higher echelon came only on January 19, 1917, when General Cristescu asked the 2nd Army, with *"Telegram no.4710"* (Romanian National Military Archives, file no. 160, f.52), to report on the veracity of what was claimed by the enemy's communications, an aspect that we have detailed above.

"Telegram no.4720" (Romanian National Military Archives, file no. 160, f. 48v) of January 20, 1917, by which the General Headquarters asked the 2nd Army to 7th Mixed Brigade to report the incident of the surrender of the 3rd Company of battalion commanded by Captain Marculescu. The telegram was coded and of a coded character secret, requesting urgent details on the incident, insisting on whether the subunit had been captured by "force majeure or good or "force of will" (sic!). The report also had to give the names of the officers responsible for the event.
The answer from the 7th Mixed Brigade also came through the 2nd Army, which sent *"Telegram no.3133"* (Romanian National Military Archives, file no. 160, f. 49) dated January 21, 1917*,* encrypted and extra-urgent, in which the entire leadership of that battalion, not only Captain Stelian Marculescu, was accused. The officers of this battalion were characterized as *"uneducated and untrained"*, and Captain Stelian

Mărculescu was accused that, on 26 December 1916, at the time of the intentional surrender on *Momâia,* he was 1 km behind the front, preparing his own meal.

The novelty of the situation is that this *Telegram* was not signed by Sturdza, but by Lieutenant-Colonel Pascu, who had taken command of the 7th Mixed Brigade after Sturdza's appointment to command the 8th Infantry Division, also part of the 2nd Army. It should be emphasized that, although the 7th Mixed Brigade had a different commander, the accusations against Mărculescu were maintained in the same vein as during Sturdza's time, a situation for which there are at least two explanations: the first, that the new commander of the brigade did not want to deviate from the "line" drawn by his predecessor, and the second, that this was simply the truth.

The cumulative effect of these two telegrams, we believe, hastened the trial of Ciulei, who, by *"Sentence No. 20/1917"* (Romanian National Military Archives, file no.11, f. 410) of the court-martial of the 2nd Army, was sentenced to death and executed on the morning of January 28, 1917. A few hours later, Crăiniceanu was caught with a packet of instigating manifestos on his person, an event that clarified Sturdza's disappearance but could not change Ciulei's fate, which was already sealed.

Justice

The administration of military justice in the War of Integration was based on the provisions of the Code of Military Justice, adopted in 1873 according to the French model, promulgated by *"High Decree no. 828 of April 5, 1873"* (Monitorul Oastei 1873) and entered into force in October of the same year. It was republished in 1881, after which it was successively amended and supplemented in 1881, 1894, 1905, 1906, 1916, and 1917, in accordance with the social, economic, and legislative changes that Romanian society had undergone, but also in an attempt to keep pace with the reality of the battlefield, with Romania's entry into the War of Integration.
The most significant amendment to the Code of Military Justice, in the economy of the present case, is the adoption of the additional Title II in the form of "*Law on the deletions, amendments, and additions to the Code of Military Justice for the time of mobilization and war*" (Official Monitor 1916, 7529-7530), registered under No. 3245 of 21 December 1916/3 January 1917.

The amendment of the Code of Military Justice, which added a Title II, was perhaps one of the most important legislative measures adopted at that time, *"an act based on military psychology"* (Zidaru 2006, 70), *and* the entire special subject matter relating to military justice was amended to take account of the *need to repress* certain acts.

It was a particularly difficult context for Romania which, at the time of the adoption of this measure, had lost, according to some authors, in the few months since the beginning of the campaign, two-thirds of the country's surface area and

approximately 250,000 soldiers, dead, wounded and missing (Torrey 2014, 352), i.e. two-thirds of the individual weapons, half of the machine guns, and a quarter of the artillery, according to other sources (Bărbulescu *et al.* 2014, 343).
The adoption of Additional Title II created the legal framework necessary to penalize new crimes, such as *treason*, *espionage*, *self-mutilation*, *causing panic in bad faith*, *creating or spreading false news*, etc., and led to the tightening of penalties, with a view to swift and exemplary repression.

The activity of *courts-martial* in times of mobilization and war was regulated by the provisions of Articles 19-35 of Title II of the Additional Title. They functioned at the headquarters of each corps, at the headquarters of independent divisions or of those operating in isolation, and wherever the exigencies of the service required.
According to the *"Instructions on Courts-Martial"* (Official Monitor 1917, 195-201), appointments to the *courts-martial* were made by the commander of the major unit with which the court-martial was functioning, each court-martial having attached to it a *royal commissioner* (prosecutor, n.s.), who also acted as a *reporter,* with somewhat similar duties to the examining magistrate.

The procedure required that convictions of military convictions, as well as convictions for treason and espionage, whether the subject was military or civilian, were immediately brought to the attention of the commander who had given the order for the court-martial, accompanied by a report from the royal commissioner.
Once approved, the sentence of the court-martial became final and enforceable by law, and was to be executed, regardless of whether the convicted person would have used the appeal remedy, given that it had been lifted by Royal High Decree no. 7 of January 10/23, 1917.
It should be emphasized that the swiftness of the court martial proceedings, together with the harsher punishments applied by the Code of Military Justice, were means of maintaining an appropriate level of discipline among the military, an imperative demanded by the constantly dynamic situation at the front.

The amendment of the Code of Military Justice overlapped with the adoption of controversial measures, such as the decree of a state of siege and the suspension of the right to appeal. The latter was adopted by King Ferdinand I after Romania entered into the war, by *"Royal High Decree No. 2930 of September 16/29, 1916"* (Official Monitor 1916, 6266), based on the provisions of Article 67 of the Code of Military Justice. This stipulated that the right of appeal for persons convicted by sentences of the councils of war could be temporarily suspended during wartime by royal decree, based on the opinion of the Council of Ministers (government, n.d.).

Royal High Decree no. 2930 was issued in the legal context of the existence of a state of siege throughout the country, instituted as a result of the circumstances created by Romania's entry into the war. The decision of King Ferdinand I was justified by the temporary nature of the measure, and was based on the report of the Minister

of War, Vintilă I.C. Brătianu, registered under no. 8257 of September 16/29, 1916, which stated: *"Sire, (...)) In the difficult times we are going through, the need to maintain military discipline firmly and to the highest degree, imperatively demands the decree of this suspension of appeals to the review board, for only in this way will the exemplary nature of the sentences pronounced by the war councils be able to produce their effect* (sic!)*, by executing them immediately after the sentences of conviction have been pronounced"* (Official Monitor 1916, 6266).

A measure "adjusted" to the difficult period that the Romanian army was going through in the 1916 campaign if we were to be guided by the date on which the supporting documents on the basis of which this High Royal Decree was issued were published in the Official Gazette.
Judging by the date of the issuance of the normative act, September 16/29, 1916, *the difficult moments* referred to in the report of the Minister of War, and which certainly contributed to the adoption of this measure, were represented by the series of military failures suffered by the Romanian army campaign up to that date.

The most resounding of these was the fall of the fortified bridgehead of *Turtucaia* on August 24/September 6, 1916, only 60 km from Bucharest, an event considered to have been *a "national catastrophe"* (Kiriţescu 1927).
It also contributed to the critical situation in Dobrogea, where the Romanian-Russian-Serb troops had lost the battle for *Bazargic* (August 25/September 7, 1916), and *Silistra* (Kiriţescu 1927, 423) had been evacuated without a fight (August 26/ September 8, 1916), the loss of the *Merișor* Pass and the mining town of *Petroșani* (September 7/20, 1916), as well as the withdrawal of *the Olt Corps* (Kiriţescu 1927, 294) under the pressure of the German army in the *Battle of Sibiului* (September 16/29, 1916).

In addition to the stated purpose of strengthening military order and discipline, the suspension of the right to appeal was also intended to raise the army's fighting capacity and to discourage any kind of demobilizing actions, given that the *appropriate measures,* according to the expression mentioned in the report, had not been established in the Ministry of Justice, but in the Ministry of War and the General Headquarters. The General Headquarters had ordered the establishment of courts-martial by *"Order of the Day No. 322 of January 12/25, 1917"* (Homoriceanu 1916, 89)*,* in the First and Second Armies, in the fifteen infantry divisions, in the two cavalry divisions, and the Fleet of Operations. Therefore, from January 12/25, 1917, 21 courts-martial, with their associated military prosecutor's offices, were in operation at the General Headquarters and the Army of Operations.

Thus, in the absence of an appeal to the Superior Court of Military Justice, the decision of the court-martial was subject to the approval of the commander of the echelon in which it was operating, and once approved it was *immediately* put into execution. After the war, this post-judgment procedure, involving the command

in the administration of justice, gave rise to the most comments and generated the greatest distrust of the objectivity, impartiality, and independence of the military justice system.

Repair

Captain Mărculescu survived both this strange incident and the war, and although wounded in the arm and neck, he somehow managed to sneak behind the Romanian front to a military hospital in Botoșani. At the time of his appearance, the Sturdza scandal was in full swing, so his status changed instantly, from *deserter* to victim of the Sturdza traitor and, implicitly, *hero*.
Was Mărculescu guilty or not? Polihroniade's accusations against Mărculescu were taken as true by Constantinescu, who wrote his own resolution on the report and forwarded it to Sturdza. These allegations were later reconfirmed by Constantinescu in his statement to the Royal Commissioner on February 28, long after Sturdza's defection had been reported.

They were also confirmed by Captain Marinescu in his statement to the Royal Commissioner, and by Lieutenant-Colonel Pascu in the report sent by telegram to the 2nd Army to be forwarded to the General Headquarters. This report, which tried to enlighten the higher echelon about the transfer of the 3rd Company to the enemy, had been drawn up a few weeks after Sturdza had handed over command of the brigade, but it conveyed the same idea: *"The battalion was badly led"* (Romanian National Military Archives, file no. 160, f. 49).

From the beginning of his career until the beginning of the war, Stelian Marculescu was characterized as a mediocre officer. The first change in his image in the eyes of his superiors can be seen in the *summary rating sheet* covering the period August 15, 1916 - August 8, 1917.
Issued under the letterhead of the 9th Infantry Regiment Râmnicu Sărat, this report sheet contains the first praise, obviously contrary to what had been recorded until then. Sărat, and the same colonel Alexandru Jecu, to whom we promised to return, commander of the 5th Infantry Division's March Regiment, former commander of Captain Stelian Marculescu, when he was in the 48th Infantry Regiment.

In the view of the new hierarchical chiefs, Mărculescu is *"energetic and presentable in front of the front, he has the eye of the field and of the unit commander, he knows the military regulations well and presents them with great precision"* (Romanian National Military Archives file no. 39, f. 25). Beyond these assessments, the fact that he is presented as the one who thwarted Colonel Sturdza's plans to desert, an episode considered by the evaluators as *"a true heroic novel"* (Romanian National Military Archives, file no. 39, f. 25), is unique, without any other details or arguments being presented.

The only one who remained consistent in his initial assessment was General Aristide Razu, who, although he seems to have compromised on Mărculescu, maintained the pre-war line and contradicted the other commanders' assessments. General Razu noted: *'Although lacking in energy, his goodwill in service compensates for his lack of military training'"* (Romanian National Military Archives, file no. 39, f. 25). The fact that, as a result of these commendatory assessments, Mărculescu was exceptionally proposed for promotion to the rank of major, and even through a special report, leads us to believe that this change of attitude towards him could have been a *moral reparation* for what happened on the evening of December 26, 1916.

The story he told to his superiors, in which he presented himself as the one who had held back the German troops that were about to break through the front in General Mannerheim's sector, and who had surprised the first attempts of treachery by Colonel Sturdza, certainly contributed to this. It was for this reason, according to the report, that Sturdza tried to escape and shot him *"and only thanks to his presence of mind (...) he escaped the bullet sent into his chest (...) as he parried the shot by lying down"* (Romanian National Military Archives, file no. 39, f. 26). No further comments!

Mărculescu was promoted to the rank of major on November 1, 1917, and in the following years, he continued to receive laudatory assessments from his regimental commander, the same Colonel Todicescu, who did not hesitate to propose in his report card for 1918-1919 that he be promoted to the rank of lieutenant-colonel, exceptionally, and that he be given command of a regiment.
These proposals were not accepted by the higher echelons, the commander of the 5th Infantry Division, General Ioan Vernescu, considering that during the period under evaluation, no circumstances had arisen that would entitle Mărculescu to be exceptionally promoted. This opinion was also shared by the commander of the III Army Corps, General Dumitru Strătilescu, former commander of the 1st Infantry Division, who had had Mărculescu under his command.

Moreover, he noted that the claim already made by the regimental commander that Mărculescu had prevented Sturdza from deserting *"is not supported by any document"* (Romanian National Military Archives, file no. 39, f. 30), *and* he was even surprised that this *claim* came from an officer, whom he considered worthy, of the caliber of Colonel Todicescu.

After 1919, Major Stelian Mărculescu's activity and training were again unfavorably evaluated. He participated with the 9th Infantry Regiment of Râmnicu Sărat in the campaign in Bessarabia, in defense of the Dniester, after which he was transferred to the Mobilization Bureau of the 48/49 Infantry Regiment of Buzău. He was promoted to the rank of lieutenant colonel on April 1, 1920, a rank with which he went into reserve in 1932.

In the summer of 1917, Second Lieutenant Constantin Ciulei was decorated (Official Monitor 1917) with the Order of *the Crown of Romania*, with swords, in the rank of *Knight*, for the bravery and courage with which he led his platoon in the Dobrogea campaign, on September 6, 1916, in the battle of *Caciamac*, *"where he captured the first line of enemy reinforcements"* (Romanian National Military Archives, file no.44, f. 05), and where he was wounded.

Captain Marculescu was also decorated (Romanian National Military Archives, file no. 44, f. 03), but following the Transylvanian campaign in the fall of 1916, with one of the highest distinctions of the Romanian state, the *Order of the Star of Romania*, with swords, in the rank of *Knight*. The distinction was awarded to him for the courage and courage with which he led his company in the battles of *Bodza-Van* (today Sita Buzăului, s.n.), where he drove the enemy out of the village after a bayonet attack and captured over 100 prisoners. Mărculescu was decorated by the same High Royal Decree (Official Monitor 1917) no. 681 of July 10, 1917, by which Ciulei had been decorated.

Coincidence or moral reparation?

We cannot know. What is certain is that the proposals for these distinctions were submitted to the Decorations Bureau of the Royal General Staff on a table of proposals initiated by the 8th Infantry Regiment Buzău, and were appropriated and supported by the commander of the 5th Infantry Division, General Aristide Razu. General Razu exercised, at least theoretically, the command of the 5th Infantry Division between December 23, 1916, and July 29, 1917, but it is possible that the actual takeover of the command of the 5th Infantry Division from General Constantin Petala was made later, perhaps even after the events of December 26, 1916, on *Momâia*.

Thus, unless General Aristide Razu marked his debut in command of the division precisely with the proposals for the promotion of Mărculescu and Ciulei, which he should have promoted within the first three days of his appointment, it is quite possible that the proposals for the decoration of the two officers were made after Ciulei's execution and Sturdza's desertion, and thus had every chance of representing, in fact, a moral reparation.

Conclusions

Thus, based on our in-depth study of the subject, as well as of the arguments that we will present below, we consider ourselves justified in believing that Sturdza is not to blame for Ciulei's death. Sturdza will go down in history as a traitor, but Ciulei's death cannot be attributed to him, even if it was he who sent him to court-martial.

In our opinion, the succession of telegrams exchanged between the General

Headquarters and the 2nd Army clearly shows the interest of the military authorities in a quick and exemplary solution to the case of the "traitor" Ciulei. Sturdza could not have such an influence in the echelon commanded by General Alexandru Averescu, but the influence of the echelon above him, the General Headquarters, not only can be considered, but the Telegram of January 21, which we have mentioned above, is even conclusive in this respect.

Thus, we can say that Sturdza could not have influenced the court-martial of the 2nd Army regarding Ciulei's trial, but the General Headquarters could have, which had suddenly become not only concerned but also interested in the subject. Having learned about the real situation of deserters and those captured by the enemy, a situation that had not appeared until then in the daily reports of the 2nd Army, the General Headquarters feared that an event like the one on Momâia, when a whole company had gone over to the enemy of its own free will, an act which resulted in the abandonment of positions and the capture of battalion-level troops, could have caused a possible contagion among the already demoralized 2nd Army troops, who were wintering at the front without the possibility of being replaced.

In our opinion, the seriousness of the acts reported by the General Headquarters did not necessarily consist in the voluntary surrender of the troop or the flight of the others from the enemy, but in the fact that on Momâia these acts were committed by a constituted subunit, together with the officers and non-commissioned officers who should have commanded it and ensured that this kind of acts did not take place. This state of affairs took place in the circumstances already described, in which even summary executions were permitted, and commanders were allowed to have the right of life and death over their subordinates.

All these measures, which we shall euphemistically call "derogatory" from the legal provisions, were adopted in the hope of maintaining order and discipline among the troops, as an alternative to military justice, a process that was considered much slower. When the same commanders chose this route, the system implemented a military justice that was insensitive to the circumstances, opaque to legal and procedural arguments, inaccessible even to elementary logic, and in which the specialized training of the officer-judges was not a priority.

Moreover, it allowed and encouraged among the members of the panels the desire to satisfy the "demands" of the high commanders, directly proportional to the level of command they exercised, to the detriment of the principle of the supremacy of law. A deeply subjective system of military justice, which gave the commanders of the echelons before which these courts-martial functioned the right to appoint judges from among their subordinate officers, and at the same time to validate their sentences.

That is the essence of this case. Regardless of how, and especially how quickly, Second Lieutenant Ciulei had been tried by court-martial, his death sentence was carried

out on January 28 only after it had been validated by the decision-makers of the 2nd Army, *the Mărdărescu - Averescu tandem*. And General Averescu had been informed since January 23/24, 1916 about the strange disappearance of Colonel Sturdza, and suspected, according to his own words, since January 27, that he had deserted.

Certainly, Sturdza's act of treachery remains just as reprehensible, but he cannot be blamed for the circumstances in which Ciulei was tried and executed. These remain the responsibility of the decision-makers of the General Headquarters and the 2nd Army, those who wanted to set an example and ordered the court-martial to put him to trial as quickly as possible, even though the minimum procedural requirements were not met, those who validated his death sentence, even though the person who had accused Ciulei was suspected of desertion. These are, in fact, *the unfortunate circumstances* mentioned at the beginning of this article, to which Second Lieutenant Constantin Ciulei fell victim, the one tried, sentenced, and executed after a sham trial, and whose guilt no longer matters.

References

Anastasiu, Ion. 1927. *Din Crimele Marelui nostru război.* Cluj: Institutul de Arte Grafice „Viața".

Averescu, Alexandru. 1992. *Notițe zilnice din război.* București: Editura Militară.

Bărbulescu, Mihai, Dennis Deletant, Keith Hitchins, Şerban Papacostea, and Teodor Pompiliu. 2014. *Istoria României.* București: Corint Internațional.

Brădișteanu, Nicolae. 1972. "„Chemarea" a răsunat în pustiu." *Magazin Istoric* octombrie nr.10 (67).

Buttescu, Mihai I. 2012. *Vânătorii Reginei Elisabeta. Memoriile unui ofițer din garda regală, ediție îngrijită de comandor (r.) Gheorghe Vartic.* București: Editura Militară.

Homoriceanu, Nicolae. 1916. *Codul Justiției Militare adnotat, Ediția a II-a.* București: Tipografia Dim.C.Ionescu.

Ioanițiu, Alexandru. 1929. *Războiul României: 1916-1918.* Vol. 1. București: Tipografia Geniului.

Kapri, Valeriu. 1926. *Cazul fostului colonel Alexandru Sturdza, comandantul Diviziei a 8-a română. Un episod din războiul mondial, 1914-1918 pe frontul român.* Oradea: Tipografia Adolf Sonnenfeld.

Kirițescu, Constantin. 1927. *Istoria războiului pentru întregirea României, 1916-1919, ediția a II-a.* București: Casei Școalelor.

Monitorul Oastei. 1873. „nr.13." *12 mai* 289-334.

Monkevitz, Nikolai A., and Aleksandr N. Vinogradski. 2019. *Aliatul inamic: descompunerea armatei ruse și pericolul bolșevizării României în 1917.* București: Editura Humanitas.

Nicolau, Eugen D. 1974. „Pe urmele unei erori judiciare: cazul sublocotenentului Ciulei." *Magazin Istoric, nr.5*, 87.

Official Monitor. 1920. "no.8 from April 15th."

___. 1916. „no.135 from September 17th."

___. 1916. "no.224 from december 28th."

___. 1917. „no.20 from April 25th."

___. 1917. "no.90 from July 16th."

___. 1917. "no.235 from January 10th."

Otu, Petre, and Maria Georgescu. 2011. *Radiografia unei trădări. Cazul colonelului Alexandru D. Sturdza.* București: Editura Militară.

Romanian Academy Library. 1919. „Avântul. Organ politic independent. Ediție de seară a ziarului Izbânda." *P.IV.4.670, 16 noiembrie.*

Romanian National Military Archives. file no.6. "Directorate of Education and Training, vol.7."

___. file no.11. "Infantry Reserve Officers Register fund."

___. file no. 21. "7th Mixed Brigade fund."

___. file no. 37. „7th Mixed Brigade fund, circular orders, agendas, telephone reports."

___. file no. 44. "Royal Staff Fund, Decorations Office."

___. file no. 924. "General Staff fund."

___. file no. 160. "Grand HQ fund."

___. file no.1691. "Grand HQ fund."

Scărișoreanu, General R. 1934. *Fragmente din războiul 1916-1918. Istorisiri documentate, Ediția a II-a.* București: Tiparul Cavaleriei.

Tăslăuanu, Octavian C. 1934. *Sub flamurile naționale. Note și documente din Războiul de Întregire al neamului.* Vol. I. Sighișoara: Editura Miron Neagu.

Torrey, Glenn E. 2014. *România în Primul Război Mondial.* București: Meteor.

Zidaru, Petrache. 2006. *Tribunalele militare, un secol și jumătate de jurisprudență (1852-2000).* București: Univers Juridic.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Counterterrorism Planning in the Shipping Industry Leveraging Competitive Intelligence

Anastasios-Nikolaos KANELLOPOULOS, Ph.D. Candidate*
Anthony IOANNIDIS, Assistant Professor**

*Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ankanell@aueb.gr
**Department of Business Administration, Athens University of Economics and Business, Greece
e-mail: ai@aueb.gr

Abstract

This paper addresses the critical need to bolster Counterterrorism (CT) strategies in the Shipping industry, which is responsible for the vast majority of global goods transportation. The objective is to advocate for the integration of Competitive Intelligence (CI) into CT planning to address current security deficiencies. Key threats such as piracy in Somalia and the Gulf of Guinea, ship-borne terrorism, and attacks on ports are examined, highlighting the limitations of existing measures like the International Ship and Port Facility Security (ISPS) Code.

The first chapter delves into primary threats, including hijacking, piracy, ship-borne terrorism, and port attacks, providing an in-depth analysis of their implications and necessary countermeasures. The second chapter explores current CT measures, focusing on the role of the International Maritime Organization (IMO) and the effectiveness of the ISPS Code, while identifying the reactive nature of existing strategies. The third chapter proposes a strategic CI framework, emphasizing comprehensive data collection, advanced analysis, threat identification, and proactive strategy development. Each component is detailed to illustrate how CI can transform CT planning, making it more anticipatory and effective.

The authors anticipate that using CI will help stakeholders, including policymakers, Shipping companies, and security agencies, adopt more proactive and effective measures against emerging threats. The proposed framework emphasizes the importance of stakeholder collaboration, public-private partnerships, and international cooperation. This study aims to enhance maritime security, ensure global trade's safe and efficient operation, and improve global maritime resilience, offering valuable insights for all industry stakeholders.

Keywords:

Counterterrorism, Shipping Industry; Competitive Intelligence;
Maritime Security; Threat Analysis.

Article info

Received: 15 November 2024; Revised: 29 November 2024; Accepted: 9 December 2024; Available online: 17 January 2025

Citation: Kanellopoulos, A.N. and A. Ioannidis. 2024. "Counterterrorism Planning in the Shipping Industry Leveraging Competitive Intelligence". *Bulletin of "Carol I" National Defence University*, 13(4): 77-87. https://doi.org/10.53477/2284-9378-24-50

The Shipping industry plays a pivotal role in global trade, handling the vast majority of the world's goods transportation (Grammenos 2010). However, its crucial function makes it a prime target for terrorist groups seeking to disrupt economic stability and create fear. Recent increases in maritime terrorism, piracy, and other illicit activities highlight the urgent need for stronger Counterterrorism (CT) strategies in the sector (Mohsendokht et al. 2024). Traditionally focused on safety and accident prevention, the industry has overlooked CT planning, leaving it vulnerable to complex terrorist threats. This paper proposes integrating Competitive Intelligence (CI) into CT strategies to enhance maritime security.

The objective is to offer a comprehensive framework for incorporating CI into security measures, empowering stakeholders – including governments, Shipping companies, and international organizations – to proactively identify and mitigate potential terrorist threats. The authors expect that adopting CI will improve risk anticipation, leading to more effective and preventive measures. This study is intended for policymakers, maritime security experts, and industry stakeholders, aiming to strengthen global maritime resilience and safeguard the international supply chain.

Key Threats to the Shipping Industry

The present chapter delves into the primary threats facing the Shipping industry, focusing on hijacking and piracy, ship-borne terrorism, and attacks on ports and infrastructure. Each section aims to provide an in-depth analysis of these threats, highlighting their implications and the measures needed to counteract them. The objective is to offer a comprehensive understanding of how these threats disrupt global trade and what can be done to mitigate their impact.

Initially, piracy, particularly off the coast of Somalia and in the Gulf of Guinea, remains a significant threat to global Shipping. Piracy off the coast of Somalia, driven by financial motives, has led to increased Shipping costs, disrupted trade routes, and heightened security concerns. The collapse of Somalia's central government in the early 2000s created a lawless environment, enabling pirates to hijack commercial vessels for ransom (Stanley and Uwizeyimana 2023). Pirates typically use small, fast boats to overtake larger vessels, demanding substantial ransoms for the release of ships and their crews. Despite international efforts to curb these activities, the financial incentives from ransoms have perpetuated the cycle of piracy (Molina et al. 2024). The persistence of Somali piracy underscores the need for robust international collaboration and sustainable solutions to address the underlying political and economic instability in the region. Continued efforts to enhance maritime security and develop local economies are crucial to mitigating this threat.

Moreover, piracy in the Gulf of Guinea is characterized by more violent and organized attacks, often involving cargo theft, kidnapping of crew members, and

armed robbery. This region, rich in oil, is a lucrative target for pirates who frequently attack oil tankers and vessels involved in the petroleum industry (Schandorf 2024). Unlike Somali piracy, which primarily involves hijacking for ransom, piracy in the Gulf of Guinea focuses on stealing cargo, particularly oil, and kidnapping crew members for ransom. The pirates in this region are highly organized, sometimes with connections to onshore criminal networks (Ahorsu et al. 2024). Further, the piracy situation in the Gulf of Guinea highlights the need for enhanced regional cooperation and stronger security measures. Addressing the socio-economic factors that fuel piracy and improving the capacity of local enforcement agencies are essential steps towards reducing this threat.

Subsequently, there is increasing concern that terrorist organizations might leverage hijacking and piracy to fund their operations or carry out ideologically driven attacks. In Somalia, the extremist group Al-Shabaab has reportedly explored maritime piracy as a revenue stream to support its insurgency efforts (Levy and Yusuf 2019). Similarly, in the Gulf of Guinea, militant groups involved in the Niger Delta conflict might turn to piracy to advance their political agendas. The potential for terrorist groups to exploit piracy for funding and operational purposes necessitates a multifaceted approach that includes CT strategies and strengthened maritime security protocols. Vigilant monitoring and international cooperation are critical to preventing such exploitation.

Furthermore, Ship-borne terrorism represents an evolving threat as terrorists increasingly consider using commercial vessels to transport weapons, explosives, or personnel. Terrorists could use the anonymity of the Shipping industry to smuggle weapons, including conventional arms, explosives, and weapons of mass destruction (WMDs), posing severe risks to coastal cities and critical infrastructure (Bueger and Edmunds 2024). Additionally, commercial ships may be used to transport personnel, including operatives planning attacks in other countries. The global nature of the Shipping industry provides cover for the movement of individuals across borders without attracting attention (McNicholas 2016; Romero 2021). The threat of ship-borne terrorism underscores the need for comprehensive security protocols and international cooperation to monitor and secure Shipping routes. Enhanced inspection procedures and intelligence sharing are vital in mitigating this risk.

Thereafter, ports serve as vital nodes in the global supply chain, making them prime targets for terrorist attacks. Attacks on major ports could have devastating economic consequences, disrupting global trade and triggering cascading effects throughout supply chains (Raymond 2006). The complexity of port operations, involving various stakeholders and handling vast amounts of cargo, presents numerous vulnerabilities that terrorists could exploit. Additionally, ports often house large quantities of hazardous materials, which can amplify the impact of an attack (Gordon et al. 2005). Cyber-attacks pose a significant threat to port operations, capable of disrupting logistics, sabotaging equipment, and compromising critical data (Kanellopoulos 2024b).

Increasing reliance on digital systems for managing logistics and coordinating vessel movements has heightened the risk of cyber-attacks. Terrorists could exploit these weaknesses to cause operational paralysis and financial losses (Kanellopoulos and Ioannidis 2024). The vulnerability of ports to physical and cyber-attacks highlights the need for comprehensive security measures and robust cybersecurity protocols. Investing in advanced security technologies and fostering international cooperation are essential to safeguarding port infrastructure.
Eventually, the Shipping industry faces numerous threats, including hijacking and piracy, ship-borne terrorism, and attacks on ports and infrastructure. Addressing these threats requires a multifaceted approach involving international cooperation, enhanced security measures, and addressing the underlying socio-economic factors that contribute to these risks.

Current Counterterrorism Measures in the Shipping Industry

This chapter explores the critical role of the International Maritime Organization (IMO) in enhancing maritime security and the measures taken by Shipping companies to protect vessels, crews, and cargoes from evolving threats. The focus is on the implementation and impact of the International Ship and Port Facility Security (ISPS) Code, the response to maritime terrorism, and the need for more proactive and intelligence-driven security strategies. The objective is to provide a comprehensive understanding of the current security landscape and the necessary steps to bolster maritime security globally.

The International Maritime Organization (IMO) has played a crucial role in implementing regulations designed to enhance maritime security on a global scale. Among the most significant of these is the International Ship and Port Facility Security (ISPS) Code, established as part of the broader International Convention for the Safety of Life at Sea (SOLAS) following the events of September 11, 2001. The ISPS Code provides a standardized framework for assessing and managing security risks in ports and on ships, outlining mandatory measures for governments, Shipping companies, and port authorities (Lloyd's Register 2024). This framework aims to deter and prevent acts of terrorism and other unlawful acts against ships and port facilities by mandating security assessments, the development of security plans, and the appointment of designated security officers. Moreover, the ISPS Code emphasizes the importance of international cooperation, requiring member states to share information and collaborate on security-related issues to protect the global maritime transportation system.

In response to the growing threat of maritime terrorism, Shipping companies have implemented various security measures aimed at protecting their vessels, crews, and cargoes (Osaloni 2023). These initiatives include the deployment of armed guards on board vessels, particularly when transiting through high-risk areas such as the Gulf of Aden and the Gulf of Guinea. Additionally, companies have adopted advanced vessel tracking systems that allow for real-time monitoring of ship movements,

enabling faster responses to potential security incidents. Crew training programs have also been enhanced, focusing on raising awareness of security threats, improving emergency preparedness, and ensuring that crew members are equipped to respond effectively in the event of an attack (Kanellopoulos 2024a, 2024c).

Despite these efforts, many of these measures are reactive in nature, primarily designed to respond to incidents after they occur rather than to prevent them. The reactive nature of many security measures limits their effectiveness, as they are often implemented after a threat has been identified or an attack has occurred. This underscores the need for more proactive and intelligence-driven approaches to maritime security (Peisl *et al.* 2021). By integrating CI and other advanced analytical tools, the industry can enhance its ability to anticipate and mitigate potential threats before they materialize. Such strategies would involve continuous monitoring of threat landscapes, sharing of intelligence across borders, and the development of predictive models that can identify potential risks in advance (Rasool et al. 2022).

While the existing international regulations and industry initiatives provide a foundational level of security within the maritime sector, they are often insufficient to address the increasingly sophisticated and evolving nature of terrorist threats. Current strategies tend to focus on compliance with regulations and the implementation of defensive measures, such as armed security and tracking systems (Okafor-Yarwood and Onuoha 2023). However, these approaches may not be adequate in a landscape where terrorist tactics are becoming more complex and unpredictable. This underscores the need for more proactive and intelligence-driven approaches to maritime security (Peisl et al. 2021). By integrating CI and other advanced analytical tools, the industry can enhance its ability to anticipate and mitigate potential threats before they materialize. Such strategies would involve continuous monitoring of threat landscapes, sharing of intelligence across borders, and the development of predictive models that can identify potential risks in advance (Rasool et al. 2022).

Ultimately, closing the gaps in current CT strategies requires a shift from reactive to proactive security measures, ensuring that the maritime industry is better equipped to prevent terrorist attacks and protect global trade. By implementing comprehensive strategies that include advanced analytics, intelligence sharing, and continuous threat monitoring, the maritime industry can enhance its resilience against evolving threats and ensure the safety and security of global maritime operations.

Integrating Competitive Intelligence into Counterterrorism Planning

This chapter delineates a strategic framework for integrating CI into CT planning within the Shipping industry. Structured around several critical steps, this framework aims to enhance the industry's capacity to detect, assess, and respond to potential terrorist threats, thereby improving the security of global maritime operations. This

introduction sets the stage for a detailed exploration of each framework component, emphasizing the importance of CI in maintaining a secure maritime environment.

- **Data Collection**: The initial step involves comprehensive data collection, which is foundational to the framework. The quality and breadth of data gathered directly impact the effectiveness of subsequent analysis and decision-making processes. To ensure a well-rounded understanding of potential threats, data should be sourced from diverse channels, including public records, intelligence reports, satellite imagery, and social media platforms (Raptis, Katsini, and Alexakos 2021). Each data stream offers unique insights, contributing to a multi-dimensional view of the threat environment. The primary objective here is to amass pertinent information to lay the groundwork for a detailed and accurate threat assessment (Klemmer et al. 2023; Rodríguez-Ibáñez et al. 2023).
- **Data Analysis**: Following data collection, rigorous analysis is crucial (Morgenthaler 2009). This process transforms raw data into actionable intelligence through advanced analytical tools and techniques such as data mining, machine learning algorithms, and predictive analytics. Each method provides unique capabilities in identifying potential security risks, thereby enhancing the ability to detect and address threats effectively.
- **Big Data Analytics**: In the CT context, big data analytics plays a pivotal role. The Shipping industry generates extensive data daily due to its vast and interconnected nature. Big data analytics enables the efficient processing and examination of this voluminous information (Saxena and Lamest 2018; Barnea 2021). Specifically, it allows for the monitoring of Shipping routes, tracking vessel movements, and analyzing communication patterns, which are crucial for identifying potential threats that might not be immediately apparent through traditional analysis methods.
- **Threat Identification and Prioritization**: Upon completing data analysis, the next step is to identify and prioritize potential threats systematically. This phase involves evaluating each identified threat's likelihood and potential impact on the Shipping industry (Yang *et al.* 2023). Prioritization is essential for efficient resource allocation, ensuring that the most significant threats receive immediate attention. By categorizing threats based on severity and probability, stakeholders can focus on mitigating the most pressing risks, thus enhancing overall security.
- **Strategy Development**: Based on the identified and prioritized threats, developing a targeted CT strategy is the subsequent step. This comprehensive strategy should incorporate measures designed to mitigate or neutralize identified threats, including implementing new security protocols, deploying additional resources to high-risk areas, and developing contingency plans for potential emergencies. The strategy must be adaptable, allowing for adjustments as new threats emerge or as the security environment evolves (Cavallo *et al.* 2020; García-Madurga and Esteban-Navarro 2020).
- **Collaboration Among Stakeholders**: Effective CT planning within the Shipping industry necessitates collaboration among a wide array of

stakeholders (Parker et al. 2017). This includes not only Shipping companies but also government agencies, intelligence organizations, and international bodies. CI serves as a critical enabler of this collaboration by providing a shared framework for threat identification, assessment, and response. Through CI, stakeholders can align their efforts, share valuable information, and coordinate their actions to enhance collective security.

- **Public-Private Partnerships**: Public-private partnerships (PPPs) are particularly vital in CT planning. The Shipping industry, primarily composed of private entities, must work closely with governmental bodies to effectively counter CT threats. PPPs facilitate the sharing of information, resources, and expertise between the public and private sectors. CI plays a central role in these partnerships by providing a common platform for data sharing and analysis, ensuring both sectors are well-informed and capable of joint action in the face of threats.
- **International Cooperation**: Given the global nature of the Shipping industry, international cooperation is indispensable for effective CT planning. This cooperation extends beyond national borders, encompassing collaboration with international organizations and regional security alliances (Seiglie and Matelly 2011). CI enhances international cooperation by offering a standardized approach to threat identification and assessment, facilitating the seamless exchange of intelligence across countries, and helping build a cohesive global response to maritime terrorism.
- **Implementation and Monitoring**: The final stage of the CI-driven CT framework involves implementing and continuously monitoring the developed strategy (Muramudalige et al. 2023). This requires deploying necessary resources, training personnel on new security protocols, and establishing monitoring systems to track the strategy's effectiveness (Gancher et al. 2023). Continuous monitoring is critical to ensure that the strategy remains responsive to evolving threats. This phase involves regular assessments and adjustments to the strategy as needed, ensuring its effectiveness in mitigating risks and protecting the Shipping industry from potential terrorist activities (Yang et al. 2023). By embedding CI into ongoing operational processes, stakeholders can maintain a dynamic and resilient CT posture capable of addressing current and emerging challenges.

In due course, integrating CI into CT planning within the Shipping industry represents a significant advancement in maritime security. By following a structured framework that includes comprehensive data collection, advanced data analysis, and proactive threat identification and prioritization, the industry can enhance its ability to anticipate and mitigate potential threats. Collaboration among stakeholders, public-private partnerships, and international cooperation further strengthen the industry's CT capabilities. Continuous implementation and monitoring ensure that strategies remain effective and adaptable to evolving threats. This proactive and intelligence-driven approach is essential for safeguarding global maritime operations and ensuring the security of international trade.

Conclusions

The present research leads to several key conclusions about the integration of CI into CT strategies in the Shipping industry.
Firstly, the study identifies critical threats to the industry, including piracy and hijacking, ship-borne terrorism, and attacks on ports and infrastructure. Piracy, particularly off the coast of Somalia and in the Gulf of Guinea, remains a significant threat, disrupting global trade and posing serious risks. The persistence of piracy in these regions underscores the need for enhanced international collaboration and sustainable solutions to address the underlying socio-economic issues that fuel such activities. Ship-borne terrorism, where terrorists use commercial vessels to transport weapons and personnel, presents an evolving threat that requires stringent security protocols and international cooperation to monitor and secure Shipping routes. Additionally, ports, as critical nodes in the global supply chain, are vulnerable to both physical and cyber-attacks. Comprehensive security measures and robust cybersecurity protocols are essential to safeguard these vital infrastructures.

Evaluating current CT measures reveals that while the ISPS Code provides a foundational security framework, its reactive nature limits its effectiveness. Similarly, industry initiatives such as deploying armed guards, implementing advanced tracking systems, and enhancing crew training programs are crucial but need to be complemented by predictive intelligence and continuous monitoring to preempt threats more effectively.

Moreover, the proposed integration of CI into CT planning involves several critical steps. Comprehensive data collection from diverse sources, followed by rigorous analysis using advanced tools, is essential for transforming raw data into actionable intelligence. Utilizing big data analytics to monitor Shipping routes, track vessel movements, and analyze communication patterns significantly enhances threat detection capabilities. Systematic identification and prioritization of threats ensure that resources are allocated efficiently to address the most significant risks.

Subsequently, developing proactive strategies involves collaboration among stakeholders, including Shipping companies, government agencies, and international bodies. CI facilitates this collaboration by providing a shared framework for threat assessment and response. Strengthening public-private partnerships and enhancing international cooperation are crucial for sharing information, resources, and expertise to counter CT threats effectively.

Furthermore, implementation and continuous monitoring of the developed CT strategies are vital. This requires deploying necessary resources, training personnel on new security protocols, and establishing monitoring systems to track the strategy's effectiveness. Regular assessments and adjustments are necessary to maintain the effectiveness of security measures. Continuous integration of CI into operational

processes ensures a dynamic and resilient CT posture, capable of addressing both current and emerging challenges in maritime security.

Summing up, integrating CI into CT strategies provides a robust framework for enhancing maritime security. By adopting a proactive, intelligence-driven approach, stakeholders can significantly improve their ability to anticipate and mitigate threats, thereby ensuring the safe and efficient operation of global trade.

References

Ahorsu, Ken, David Suaka Yaro, and Derrick Attachie. 2024. "Maritime Piracy and Its Implications on Security in the Gulf of Guinea." *Eastern African Journal of Humanities and Social Sciences* 3 (2): 1–10. https://doi.org/10.58721/eajhss.v3i2.470.

Alam Muhammad Mahtab, Yannick Le Moullec, Rizwan Ahmad, Maurizio Magarini, and Luca Reggiani. 2020. "A Primer on Public Safety Communication in the Context of Terror Attacks: The NATO SPS 'COUNTER-TERROR' Project." NATO Science for Peace and Security Series, January 19–34. https://doi.org/10.1007/978-94-024-2021-0_3.

Barnea, A. 2021. "Big Data Can Boost the Value of Competitive Intelligence." *Competitive Intelligence Magazine, 26* (1). https://www.scip.org/page/Big-Data-Boost-Competitive-Intelligence.

Bueger, Christian, and Timothy Edmunds. 2024. *Understanding Maritime Security*. *Oxford University Press EBooks*. Oxford University Press. https://doi.org/10.1093/oso/9780197767146.001.0001.

Carvalho, P. S. de. 2021. "Fundamentals of Competitive Intelligence (CI) - Paulo Soeiro de Carvalho – Medium." *Medium.* https://paulosoeirodecarvalho.medium.com/fundamentals-of-competitive-intelligence-ci-1-ebf07520746e.

Cavallo, Angelo, Silvia Sanasi, Antonio Ghezzi, and Andrea Rangone. 2020. "Competitive Intelligence and Strategy Formulation: Connecting the Dots." *Competitiveness Review: An International Business Journal* ahead-of-print (ahead-of-print). https://doi.org/10.1108/cr-01-2020-0009.

Galgano, Francis A. 2024. "Hostis Humani Generis: Pirates and Global Maritime Commerce." *Research in Globalization* 8 (June): 100188. https://doi.org/10.1016/j.resglo.2023.100188.

Gancher, Joshua, Sydney Gibson, Pratap Singh, Samvid Dharanikota, and Bryan Parno. 2023. "Owl: Compositional Verification of Security Protocols via an Information-Flow Type System," 2023 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2023, pp. 1130-1147. https://doi.org/10.1109/sp46215.2023.10179477.

García-Madurga, Miguel-Ángel, and Miguel-Ángel Esteban-Navarro. 2020. "A Project Management Approach to Competitive Intelligence." *Journal of Intelligence Studies in Business* 10 (3). https://doi.org/10.37380/jisib.v10i3.636.

Gordon, Peter, James E Moore, Harry W Richardson, and Qisheng Pan. 2005. "The Economic Impact of a Terrorist Attack on the Twin Ports of Los Angeles–Long Beach". https://doi.org/10.4337/9781845428150.00019.

Grammenos Costas. 2010. The Handbook of Maritime Economics and Business. Taylor & Francis.

International Maritime Organization (IMO). 2020. International Ship and Port Facility Security (ISPS) Code.

Lloyd's Register (LR). 2024. *International Ship and Port Facility Security (ISPS) code.* https://www.lr.org/en/services/statutory-compliance/isps-code/.

Kalogeraki, Eleni Maria, Spyridon Papastergiou, Nineta Polemi, Christos Douligeris, and Themis Panayiotopoulos. 2018. "Exploring Cyber-Security Issues in Vessel Traffic Services." *Knowledge Science, Engineering and Management*, 442–51. https://doi.org/10.1007/978-3-319-99365-2_39.

Kanellopoulos, Anastasios-Nikolaos. 2024a. "Counterintelligence Risks in Crew Management and Recruitment: The Role of Profiling and Screening in Shipping Companies." *Bulletin of "Carol I" National Defence University* 13 (2): 44–59. https://doi.org/10.53477/2284-9378-24-19.

Kanellopoulos, Anastasios-Nikolaos. 2024b. "Enhancing Cyber Security and Counterintelligence in the Shipping Industry." *National Security and the Future* 25 (1): 137–54. https://doi.org/10.37458/nstf.25.1.6.

Kanellopoulos, Anastasios-Nikolaos. 2024c. "Insider Threat Mitigation through Human Intelligence and Counterintelligence: A Case Study in the Shipping Industry." *Defense and Security Studies* 5 (March): 10–19. https://doi.org/10.37868/dss.v5.id261.

Kanellopoulos, Anastasios-Nikolaos and Ioannidis, Anthony. 2024. "Leveraging competitive intelligence in offensive cyber counterintelligence: An operational approach for the Shipping industry." *Security and Defence Quarterly*, 48 (4). https://doi.org/10.35467/sdq/192342.

Klemmer, Konstantin, Esther Rolf, Caleb Robinson, Lester Mackey, and Marc Rußwurm. 2023. "SatCLIP: Global, General-Purpose Location Embeddings with Satellite Imagery." *ArXiv (Cornell University)*, January. https://doi.org/10.48550/arxiv.2311.17179.

McNicholas, Michael A. 2016. "Targeting and Usage of Commercial Ships and Port by Terrorists and Transnational Criminal Organizations," 261–79. Butterworth-Heinemann. https://doi.org/10.1016/B978-0-12-803672-3.00008-X.

Mohsendokht Massoud, Huanhuan Li, Christos Kontovas, Chia-Hsun Chang, Zhuohua Qu, and Zaili Yang. 2024. "Enhancing Maritime Transportation Security: A Data-Driven Bayesian Network Analysis of Terrorist Attack Risks." *Risk Analysis*, July. https://doi.org/10.1111/risa.15750.

Molina, Renato, Juan Carlos Villaseñor-Derbez, Gavin McDonald, and Grant R McDermott. 2024. "Dangerous Waters: The Economic Toll of Piracy on Maritime Shipping." *SSRN Electronic Journal*, January. https://doi.org/10.2139/ssrn.4811789.

Morgenthaler, Stephan. 2009. "Exploratory Data Analysis." *Wiley Interdisciplinary Reviews: Computational Statistics* 1 (1): 33–44. https://doi.org/10.1002/wics.2.

Muramudalige, Shashika R, Hung, Benjamin, Rosanne Libretti, Jytte Klausen, and Jayasumana, Anura P. 2023. "Investigative Pattern Detection Framework for Counterterrorism." https://arxiv.org/abs/2310.19211.

Okafor-Yarwood, Ifesinachi Marybenedette, and Freedom C. Onuoha. 2023. "Whose Security Is It? Elitism and the Global Approach to Maritime Security in Africa." *Third World Quarterly* 44 (5): 1–21. https://doi.org/10.1080/01436597.2023.2167706.

Osaloni, Oluwatosin S. 2023. "The Legal Frameworks Arising from Using Armed Guards Onboard Ships: Challenges and the Way Forward." Beijing Law Review 14 (02): 621–33. https://doi.org/10.4236/blr.2023.142032.

Parker, David, Julia M. Pearce, Lasse Lindekilde, and M. Brooke Rogers. 2017. "Challenges for Effective Counterterrorism Communication: Practitioner Insights and Policy Implications for Preventing Radicalization, Disrupting Attack Planning, and Mitigating Terrorist Attacks." Studies in Conflict & Terrorism 42 (3): 264–91. https://doi.org/10.1080/1057610x.2017.1373427.

Peisl, Thomas, Joanne Hyland, Richard Messnarz, Bruno Wöran, Samer Sameh, Georg Macher, Jürgen Dobaj, Laura Aschbacher, and Detlev Aust. 2021. "Innovation Agents – Moving from Process Driven to Human Centred Intelligence Driven Approaches." Communications in Computer and Information Science, January 319–35. https://doi.org/10.1007/978-3-030-85521-5_21.

Raptis, George E, Christina Katsini, and Christos Alexakos. 2021. "Towards Automated Matching of Cyber Threat Intelligence Reports Based on Cluster Analysis in an Internet-of-Vehicles Environment," July. https://doi.org/10.1109/csr51186.2021.9527983.

Rasool, Abdur, Chayut Bunterngchit, Luo Tiejian, Md. Ruhul Islam, Qiang Qu, and Qingshan Jiang. 2022. "Improved Machine Learning-Based Predictive Models for Breast Cancer Diagnosis." International Journal of Environmental Research and Public Health 19 (6): 3211. https://doi.org/10.3390/ijerph19063211.

Romero, J. 2021. "Prevention of Maritime Terrorism: The Container Security Initiative." Chicago Journal of International Law. 2021. https://www.semanticscholar.org/paper/Prevention-of-Maritime-Terrorism%3A-The-Container-Romero/ba5b4fa70728bd8ea8b90dd014d2867acb186c2c?utm_source=consensus.

Saxena, Deepak, and Markus Lamest. 2018. "Information Overload and Coping Strategies in the Big Data Context: Evidence from the Hospitality Sector." Journal of Information Science 44 (3): 287–97. https://doi.org/10.1177/0165551517693712.

Schandorf, Stephanie Oserwa. 2024. "Reimagining Counter-Piracy Efforts in the Gulf of Guinea: Lessons from the Theory of Infrastructure for Coordination and Information Sharing*." African Security Review, August 1–17. https://doi.org/10.1080/10246029.2024.2373110.

Seiglie, Carlos, and Sylvie Matelly. 2011. "Economics of Peace and Security -Global and Regional Security Alliances -Carlos Seiglie and Sylvie Matelly ©Encyclopedia of Life Support Systems (EOLSS) GLOBAL and REGIONAL SECURITY ALLIANCES." https://www.eolss.net/sample-chapters/c13/E6-28A-04-03.pdf.

Stanley Osezua Ehiane, and Dominique Uwizeyimana. 2023. "Exploring Maritime Piracy and Somalia National Security." International Journal of Membrane Science and Technology 10 (2): 3128–37. https://doi.org/10.15379/ijmst.v10i2.3068.

Yang, Yiling, Tiantian Gai, Mingshuo Cao, Zhen Zhang, Hengjie Zhang, and Jian Wu. 2023. "Application of Group Decision Making in Shipping Industry 4.0: Bibliometric Analysis, Trends, and Future Directions." Systems 11 (2): 69. https://doi.org/10.3390/systems11020069.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Rethinking military command and control systems

LTC George-Ion TOROI, Ph.D.*

*"Carol I" National Defence University, Bucharest, Romania
e-mail: george_toroi@yahoo.com

Abstract

The evolution of society and the new characteristics of armed conflict, as demonstrated in today's wars, highlight the need to adapt the military system to meet current and future challenges. In an increasingly complex and contested operational environment, command and control systems must be the first priority in this endeavour because of their impact on all other components of the military domain. Moreover, the technologization of society and the increased transparency of the confrontational environment place additional pressure on ensuring the effective protection and functionality of command-and-control systems.

This article explores the need to rethink the architecture and fundamentals of C2 systems, analysing the essential elements that support operational effectiveness: flexibility, modularity, survivability, small footprint and resilience. In the context of new multi-domain operational paradigms and accelerated technological progress, C2 adaptation involves the integration of emerging technologies such as artificial intelligence, automation and real-time response capabilities to optimize decision-making. In particular, it emphasizes the importance of modularity and redundancy to ensure the operation of systems under conditions of intense conflict, as well as reducing electromagnetic vulnerability and increasing mobility. The article's conclusions propose practical solutions for adapting C2 systems organized around the four components of people, processes, technology systems and command posts, highlighting their essential role in achieving decision advantage, a critical element of operational success on the modern battlefield.

Keywords:

C2 (command and control); decision; adaptation; technology; human factor.

Article info

Received: 4 November 2024; Revised: 15 November 2024; Accepted: 2 December 2024; Available online: 17 January 2025

Citation: Toroi, G.I. 2024. "Rethinking military command and control systems".
Bulletin of "Carol I" National Defence University, 13(4): 88-112. https://doi.org/10.53477/2284-9378-24-51

Today's operational environment is evolving into an integrated conglomerate of threats, assets and capabilities, extending beyond the traditional land, air and maritime domains into space, cyber, the electromagnetic spectrum or the information dimension. This increased complexity requires rethinking the way military operations are planned, conducted and managed, and poses new challenges to traditional command and control concepts. Against the backdrop of profound changes in the defence sector, but also against the backdrop of increasing great power competition, Western militaries are taking accelerated steps to adapt to the new demands and opportunities of contemporary armed conflict (Bailey 2023).

Modern approaches such as multi-domain operations, a concept developed by the US Army and also implemented by NATO, can provide solutions to these new requirements, demonstrating the need for greater convergence of capabilities and synchronization across the different domains of operations, but also with international partners. The challenges posed by major technological adversaries such as China and Russia underline the urgency of adapting armed forces to a new type of great power competition across the spectrum of conflict. This transition is not limited to matching military capabilities but involves a broad process of integrating advanced technologies, from artificial intelligence and automatization to satellite surveillance and digitized communications.

Research problem

In this context, rethinking command and control systems becomes a strategic imperative for any actor. However, implementing these changes is not without difficulties, as the evolving operational environment places multiple and often conflicting demands on these systems. This article analyses the implications of these changes for the Romanian Armed Forces, as the main target of this study, and explores possible directions for adapting command and control systems in an attempt to shape a viable command model in the face of the complex challenges of the future.

Research objective

For this reason, this paper aims to analyse the factors influencing C2 systems and to identify courses of action for the main target of this study, the Romanian Army, in its efforts to adapt to current and near-future challenges. The need for such an endeavour comes against the backdrop of changes in the way armed conflicts are understood and conducted, as well as the accelerated development of technological systems and their impact on the current mode of operation. Furthermore, given the importance of command and control as a central element in the process of military operations, it is imperative that the armed forces' approach to adaptation begin with an analysis of command-and-control systems.

Research methodology

The research carried out was **a qualitative** one, aimed firstly at understanding the specific nuances of command-and-control systems, and then at analysing the

challenges they face as a result of the nature and character of the conflicts and the trends in the evolution of the operating environment. In line with the qualitative approach adopted, we also opted for **inductive reasoning**, constructing our conclusions and findings from the available empirical data (Leavy 2023, 9; Creswell and Creswell 2023, 276).

Given the qualitative nature of the study, it did not aim to test and validate hypotheses. The paper was guided by the following **research questions:**

- What are command and control systems?
- What factors influence command and control systems?
- What aspects need to be taken into account for an effective adaptation of command-and-control systems?

The logical scheme of the research undertaken is shown in the figure below.

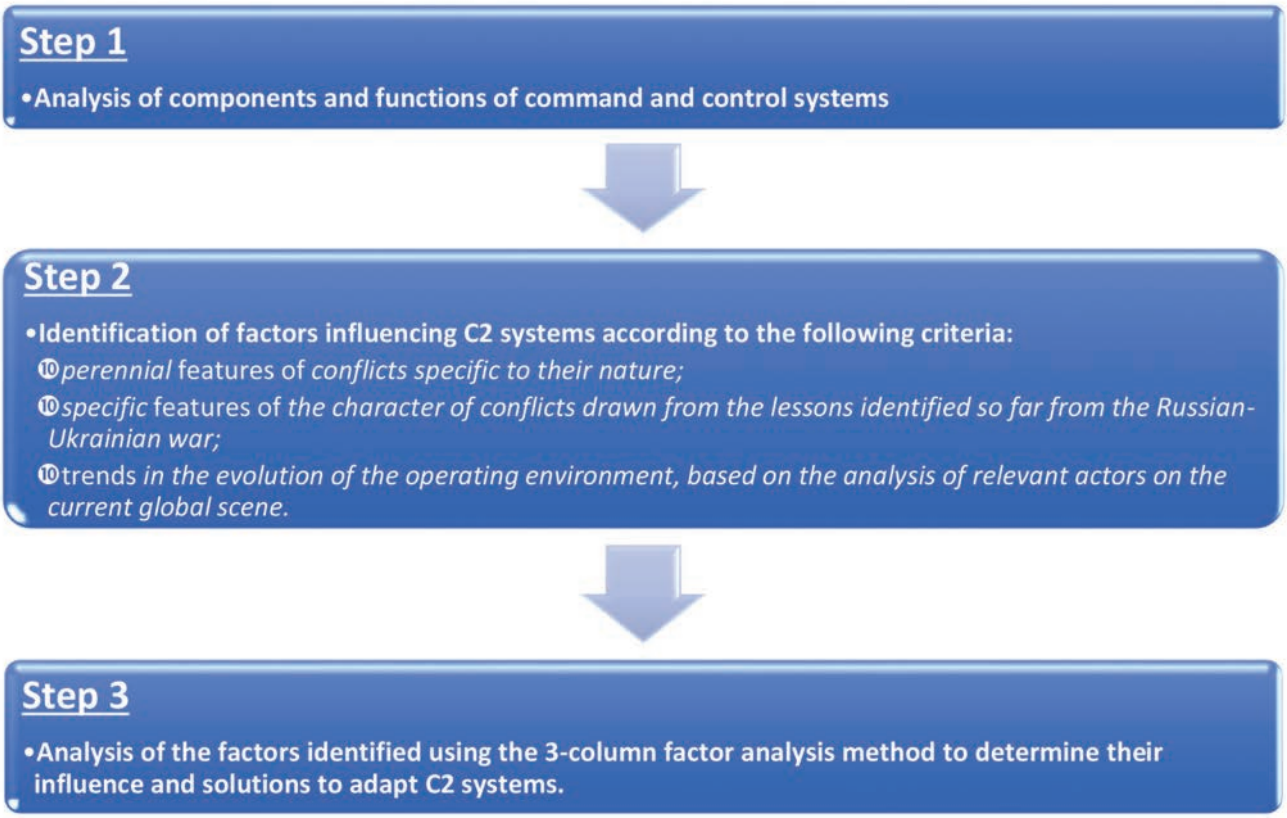


Figure 1 Logical scheme of the research
Source: author's conception

Figure no 1 - Both **primary and secondary data** were employed. For example, we used the results of previous research to identify those elements of the enduring nature of the conflict, its character as a result of the Russian-Ukrainian war, and the evolving trends in the operational environment that may affect command and staff systems. We collected these data using the method of documentary analysis to select

those most relevant to the purpose of the study and the research questions. **The sampling** of these data **was non-probabilistic** and based on three secondary data selection criteria:

- the perennial characteristics of conflicts, which are specific to their nature;
- the specific features of the nature of conflicts, based on the lessons learned so far from the Russian-Ukrainian war;
- the trends in the development of the operating environment, based on the analysis of the relevant actors on today's global scene.

The primary data used resulted from a proprietary process of inference on the results obtained from the analysis of the impact of the factors identified in relation to the three previous criteria on C2 systems, using the **individual brainstorming method**. The factors resulted from the application of the **comparative analysis method** to the previously selected documents to ensure their operational relevance.
In the final phase of the research, the **thematic analysis method** was used to identify the aspects necessary for the adaptation of command-and-control systems, coding the data and organizing them into the four specific components of any C2 system: people, processes, technological systems and command posts.

We do, however, recognize several **limitations to the results of our study**, arising either from the unclassified nature of the data used or from the methodological approach adopted. Given the high degree of researcher involvement in the conduct of the study, we were always aware of potential biases that could have influenced the results obtained, and we constantly took reflexive steps to reduce their influence.

Structure of the paper
The paper was divided into three main parts in order to answer the three research questions. Thus, in the first stage, we analysed the characteristics, components and functions of command-and-control systems, highlighting their operational relevance. In the second part, which is also the focus of the paper, we analysed the factors and how they can influence the functioning of the systems, as well as ways to counteract them from a C2 perspective. In the last section, dedicated to conclusions and proposals, we organized the results of the previous section according to the four components of any command-and-control system: people, processes, technological systems and command posts, and proposed relevant and coherent directions for their adaptation for the Romanian Army.

1. Operational relevance of command-and-control systems

For as long as humanity has existed, conflict has been a constant, reflecting the most violent expression of societies. Developing philosophies to manage them, to create the conditions necessary to ensure victory has been a constant human endeavour.
Nowadays we find ourselves at a turning point for everything that is the military

instrument of power. In an increasingly complex and dynamic environment (MCDC 2020, 1-2; TC 7-102 2014, 1-2; JCN1/17 2017, 1), the ability to ensure the operational coherence of forces has become critical to the success of military missions. Within this framework, it is necessary to develop and field advanced command and control (C2) systems to provide the engine for transforming the military system to meet the challenges of the operational environment. C2 systems are the operational core of a modern military force, enabling effective coordination of resources and rapid decision-making in critical situations, and are essential for the efficient and effective planning and execution of combat operations. These systems must be adaptable to rapid changes in the current operational environment and provide a complete picture and accurate understanding of the operational situation.

No activity in a military system is more important than command and control (MCDP-6 2018, 1-3). While it may not be able to carry out direct attacks on the enemy, influence the enemy's perceptions or provide the logistical support necessary for its own combat structures - all of which are critical to the success of military operations - none of these activities would be possible without command and control.

Although command-and-control is discussed in the literature (AJP-3 2019, 1-21 - 1-25) alongside the other functions of warfare, such as intelligence, manoeuvre, fire support, information activities, protection or logistic support, in reality, none of these functions would have a clear purpose without command and control. It encompasses all military functions and operations, giving them meaning and harmonizing them into a meaningful whole. For this reason, command and control systems are of paramount importance in a military context, ensuring the coordination and effectiveness of the actions undertaken by the armed forces. A thorough understanding of these systems is therefore critical to the success of military operations.
Command and control is the authority, responsibility and activities of military commanders in the effective direction and coordination of military forces and in the execution of orders relating to the preparation and conduct of military operations (ATP 3.2.2 2016, 1.1).

The commander is a critical element of the command-and-control system. His or her role is to oversee and direct a wide range of activities, including operational planning, organizing and directing resources, assessing threats, making decisions, and supervising and training troops. Through command and control, he ensures the cohesion and synchronization of military action, enabling the achievement of set objectives and effective mission accomplishment. A well-developed command and control system optimizes the use of resources, improves decision-making and enhances the ability to respond to critical situations. Command-and-control is, therefore, an essential element in the success of any military operation.
Although the central element of C2 is the commander, he or she cannot command and control forces and operations alone but needs support. Command-and-control,

therefore, involves more than the commander. The people involved, the processes used, the technological systems or the facilities from which it can be exercised (command posts) are elements of similar importance, as shown in Figure 2. It is impossible to talk about effective C2 without considering these four elements in addition to the commander. In the following lines, we will briefly analyse what each of them entails, in order to provide the framework for the analysis in the following sections on the adaptation needs of command-and-control systems.

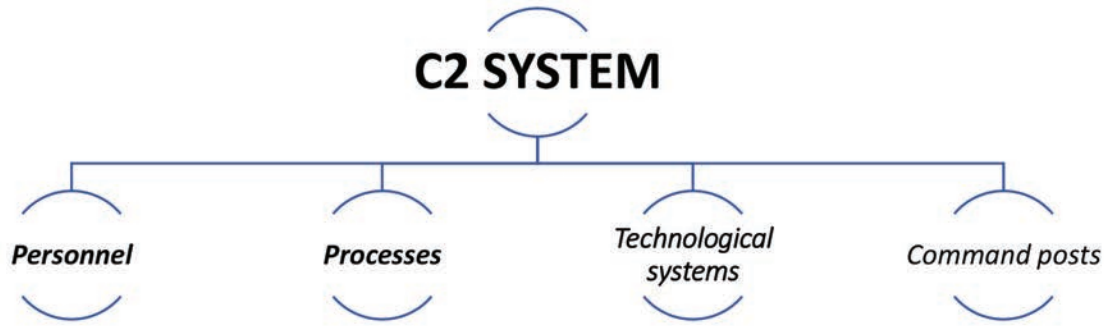


Figure 2 Command and control system elements (Wade 2023, 3-8)

From a C2 perspective, **personnel (Pe)** plays a key role in the effectiveness and coherence of the command-and-control system. Commanders, as mentioned above, are the central element in this process, having direct responsibility for decision making and command of forces. In addition, their authority and leadership style can make a significant contribution to enhancing the morale component of the combat power of armed structures (AJP-3.2 2022, 18). Their mere presence in certain moments and areas of battle can often have a decisive impact on the outcome. Historical examples abound to support this assertion. Given their crucial role in directing the course of operations and, consequently, the conduct of the conflict, commanders must manage their time between the CPs and the positions of subordinate units in order to understand the situation, observe operations and their effects at first hand, and motivate subordinates by personal example.

However, it is physically impossible for these measures alone to provide a comprehensive understanding of the operational situation. Time is a major constraint on the ability of commanders to be present throughout the theatre of operations. For this reason, the role of staff officers is extremely important. They must support commanders in making and implementing decisions by providing analysis and assessments in their specific functional areas that increase the effectiveness of the commander's decisions. Staff personnel are responsible for preparing plans, orders and assessments to ensure effective control of operations. They also contribute to the integration and synchronization of combat power by providing relevant information to facilitate situational awareness and mission progress.
When analysing the command-and-control system, emphasis should be placed on elements such as management style, leadership, or the way in which forces are

trained and educated to improve the performance of personnel involved in specific command-and-control system processes.

The second component of C2 systems are specific **processes (Pr)**. They are an essential element in the organization of activities within major nations. Coherent integration of these processes to facilitate timely decision-making and support effective coordination of combat resources and actions is achieved through the development of a well-articulated battle rhythm, integrated with that of the higher echelon and subordinate structures. Command and control processes play a vital role in ensuring the operational effectiveness of military systems. They enable the coordination and synchronization of actions during a military operation and contribute to its success. A crucial aspect of these processes is that they can provide the military structure with the framework to anticipate and respond rapidly to changes in the operational environment.

A key process is the operational process, which encompasses the core command and control activities carried out during the planning, preparation, execution and ongoing evaluation phases of the operation. This framework enables commanders to understand the operational environment, visualize and describe the end state of the operation, make articulated decisions and direct subordinate structures to achieve their own intent for how the operation should be conducted (ADP 6-0 2019, 2-14 - 2-16).

In addition to the operational process, commanders and staffs use integrative processes to synchronize various specific functions. These processes consist of a series of steps and activities that integrate warfighting functions by involving multiple disciplines to achieve a specific objective. Integrative processes include information preparation of the operational environment, intelligence gathering, targeting, risk management or knowledge management.

C2 processes are designed to be simple and fast, allowing commanders to operate effectively even under extreme stress. They must be efficient enough to increase the pace of operations and simplify staff planning sequences to facilitate rapid response. In addition, C2 processes must provide flexibility and adaptability in the face of changing circumstances and allow for continuous improvement to meet the increasingly complex challenges of the operational environment. Thus, the optimal implementation and exploitation of C2 processes can ensure efficient workflow and effective resource management in order to achieve the set operational objectives.

However, given the digital age we live in and the increased dynamics of operational change, commanders need advanced tools and technologies to enhance their ability to make real-time decisions and communicate them effectively and in a timely manner. For this reason, the third component of command and control, **technological systems (TS)**, is essential to ensure effective communication between the different levels of command and control, as well as to monitor and manage military resources in the

best possible way. The development and implementation of modern technologies and high-performance information systems are therefore essential to ensure the effectiveness and speed of military command and control processes.
The main components of technology systems include end-user applications, information services and data, and transport and digital information management. These elements work together to ensure efficient communication and information management, supporting the effective operation of the C2 system.

Time is a critical factor in modern military operations. Armed forces must work hard to ensure that they execute the action-decision cycle, also known by its inventor's name, the Boyd cycle (OODA - Observe, Orient, Decide, Act), faster and more accurately than the adversary. In this context, the ability to use technology to accelerate timely decision-making can ensure a decision advantage over the adversary.

The final component of the C2 system is the **Command Posts (CPs)**, which play a key role in ensuring the continuous coordination, synchronization and exchange of information between different structures. Their importance stems from the fact that they provide a physical location where people, processes and technological systems are integrated to assist commanders in understanding, visualizing, describing, directing, controlling, executing and evaluating military operations.

Functions common to all command posts include managing knowledge and information, developing and maintaining an accurate understanding of the situation, maintaining current assessments to support the commander's decision-making, controlling ongoing operations, evaluating ongoing operations and planning for the next phases of combat, and coordinating with internal and external organizations in the interest of accomplishing the assigned mission.

All these four elements are essential to the effectiveness of the command-and-control system. The ability to create a C2 system that outperforms the adversary's is a vital step in realizing the preconditions for operational success (ATP 3.2.2 2016, 1.1). In this approach, it is mandatory to identify solutions to streamline the **specific functions of any C2 system**:

- *developing accurate and timely situational awareness* – providing accurate and timely information about the enemy, terrain and own vulnerabilities;
- *developing clear and flexible objectives* – adjusting objectives as the situation changes;
- *establishing situationally appropriate actions* – directing and coordinating the efforts of forces for a harmonized and forceful action;
- *providing continuous monitoring* – so as to enable rapid adaptation to changes on the battlefield;
- *ensuring operational security* – so as to prevent the enemy from gaining information about the true intentions of his own forces;

• *generating a high tempo of action* - exploiting opportunities and ensuring a high tempo of military action to maintain the operational initiative.

2. Contemporary operational challenges to command-and-control systems and potential adaptation solutions

The purpose of this chapter is to identify the factors that may affect command and control in the current operational environment, an approach that is extremely important in determining the potential actions to be taken to adapt command and control systems. In addition, this section aims to draw inferences and conclusions relevant to command-and-control systems in relation to the factors identified, using a critical tool often used in the military operational planning process, the three-column factor analysis.

I would like to mention at the outset that the factors we have analysed in this chapter have only resulted from the analysis of open, publicly available, unclassified sources. In doing so, we acknowledge one of the main limitations of the results of the study undertaken, which results from the nature of the data collected and analysed. The sampling of the data used was non-probabilistic and was carried out in relation to three elements that we consider relevant to the process of adaptation of command-and-control systems:

- perennial features of conflicts specific to their nature;
- the specific features of the character of conflicts drawn from the lessons identified so far from the Russian-Ukrainian war;
- the trends in the evolution of the operating environment based on the analysis of relevant actors on the global scene today.

2.1. Analysing the nature of conflicts in terms of their influence on C2 systems

War is a social phenomenon, the most violent expression of society at any given time. According to most military theorists, it contains both some characteristics that have remained constant over the years and others that have changed with history. The nature of war is the timeless component; it is neither defined by when it takes place nor by the characteristics of the society at that time. Therefore, we can say that it has remained constant over time. Certain fundamental aspects of warfare, such as the role of the human factor, the violent nature of confrontations, their destructive impact on societies, and the constant uncertainty or friction, have remained constant over time and are considered to be essential features of warfare, regardless of how they will change. While all of these characteristics influence C2 systems to some extent, the greatest influence is undoubtedly **the level of uncertainty** specific to military confrontations. How it affects C2 systems, and possible solutions to limit its negative impact, can be found in the analysis in the table below.

TABLE NO. 1

Analysis of the level of uncertainty specific to the nature of armed conflict from the perspective of command and control systems

Factor 1 – *Level of uncertainty specific to the nature of armed conflicts*	
Deductions	**Conclusions**
1.1. Influencing decision-making (Increased risks)	**1.1.1. Decision-making under uncertainty (Pr, Pe)** - training staff in calculated risk acceptance and operational risk management; - effective integration of risk management into decision-making. **1.1.2. Developing staff critical thinking (Pr)** - use of analytical tools for analysing information (e.g. Red teaming, Alternative Analysis, etc.); - educating staff in the use of critical and creative thinking.
1.2. Difficulties in anticipating how the operational situation will evolve	**1.1.2. Opportunities to mislead the opponent (Pr)** - using uncertainty as a basis for constructing an operation to mislead the adversary. **1.2.1. The need to invest in emerging technology to enhance data collection and analysis capabilities. (ST, Pr)** - integration of emerging technology (e.g. Artificial Intelligence) in support of specific processes to achieve operational insight.

2.2. Analysing the nature of conflicts in terms of their influence on C2 systems

Although some aspects of conflict remain unchanged over time, as outlined above, it is the character of war that is constantly evolving. It has changed almost radically over time, depending on the circumstances at the time of the conflict. The main drivers of change are society, diplomacy, politics and technology (JP-1 2017, I-4). This metamorphosis of armed conflict thus depends primarily on technological and scientific innovations, demographic, political and even educational changes in a society at a given time, and to a large extent on the specific characteristics of the security environment at that time (UK Ministry of Defence 2020, 1).

In today's highly complex and rapidly changing world, command and control systems must keep pace with and adapt to these changes in order to maintain the viability of their essential functions for the effective conduct of combat operations. The first defining characteristic of contemporary society is its increasing **technologization** and the growing dependence of the human factor on such technologies, and the military domain is no exception. This presents a number of opportunities but also challenges for future C2 systems.

The ability to make decisions faster and more accurately than the enemy, coupled with advances in the accuracy of long-range weapons and reduced time to engage targets, are critical advantages on the modern battlefield. Current technology is having a profound impact on all branches of the military, "driving the adaptation of military art and existing doctrines, manuals and operational procedures". (Stanciu and Gimiga 2023, 159) Whether it is the process of detecting and engaging targets, gathering and analyzing intelligence, or communicating and maintaining the operational picture, technology has fundamentally changed the way armed forces operate and, by extension, command and control systems.

Technological development has also led to an expansion of the specific domains in which armed forces operate, with NATO's relatively recent recognition of cyberspace

and cyber warfare. As a result, armed confrontations have become much more complex, with multi-dimensionality being one of their most striking characteristics. Today, we talk about the need for a **multi-domain approach** to military operations in order to accomplish the missions entrusted to them. (Crilly and Mears 2022; Ellison and Sweijs 2023, 1; NATO 2022; NATO Parliamentary Assembly 2022, 3). Such an approach poses additional challenges for C2 systems, which must adapt to the complexity and integration of information from different domains (land, air, sea, cyber, and space).

In addition, the rapid development of **anti-satellite technology** and the increased ability to conduct extended hostile **operations in cyberspace** have added significant new dimensions to an already complex picture of how a possible future great power conflict might unfold (Nilsson 2023, 49). All of this has a direct impact on command-and-control systems, as today's armed forces rely heavily on satellites for navigation, communications, surveillance and reconnaissance, the loss of which could severely compromise the ability to coordinate, synchronize and execute operations across multiple theatres of operation. In addition, hostile operations in cyberspace have become increasingly sophisticated and widespread in recent years. These may include attacks on critical infrastructure, such as energy, transport, banking or defence systems, with the potential to have a significant impact on the effectiveness and security of C2 systems.

In addition, as a direct result of increased technological development, we are witnessing an increase in the technical capabilities of military sensors to collect information. This has led to greater transparency on the battlefield. A key element in supporting this, as demonstrated by the Russian-Ukrainian war (Gosselin-Malo 2024), is the use of drones. "The use of unmanned aerial systems has created a transparent battlefield in which there is no hiding place". (Collins 2023, 8)

Drones have revolutionized the way armed forces operate. Their versatility makes drones an extremely important weapon with the potential to support multiple combat functions. Originally used only for reconnaissance, drones have become lethal strike weapons for much more expensive armoured technology. Their operational relevance is evidenced by the nickname given to them in the literature: magic bullets (Hambling 2020). Their impact on command-and-control systems is also extremely high. Ensuring the protection and security of command-and-control centres is one of the greatest challenges facing an adversary's unmanned aerial systems. However, drones also have an extremely important role to play in supporting the development of deep situational awareness: "The information provided by drones and distributed through new digital battlefield command networks greatly increases the speed of decision and action". (Molloy 2024, 90)

Western militaries have enjoyed a superior position in all conflicts since the beginning of this millennium, but this is no longer the case. The world is in a state

of fierce competition, with **multipolarity** being the fundamental characteristic of today's society (IISS 2023, 27). The current situation demonstrates that the ability to operate freely with access to most technological and operational facilities is no longer valid. **The operating environment is highly contested**, with potential adversaries possessing qualitatively similar capabilities. This puts additional pressure to rethink command and control systems, from the specific processes to the technology used or the way command posts are organized. The classic format of the latter, specific to the conflicts of the early millennium, highly static, impressively large and with technology at their disposal, make these command posts a relatively easy target in the face of an extremely powerful adversary such as those of today (Nagl 2024, p. 24). Reducing and masking size, thermal and electromagnetic footprints, or increasing mobility **must be mandatory steps to ensure the survival of command-and-control systems** in today's operational environment (Beagle, Slider and Arrol 2023, 10). In addition, **increasing the accuracy and lethality of weapons, as well as the transparency of the battlefield and the reduction in the time required to identify and engage targets**, pose additional challenges to these systems and require the identification of viable solutions to enhance the protection of command posts in order to ensure the continued functionality of military structures and the operations they conduct.

The increasing pace and complexity of military operations is also a key challenge today. Improvements in mobility, range and lethality are compressing the boundaries of time and space, requiring greater amounts of up-to-the-minute information and an increased operational tempo, putting additional pressure on the effective performance of certain command and control system functions. In addition, the increasing lethality of weapons requires forces to be more widely dispersed to ensure their survivability, pushing the limits of command-and-control systems and requiring a significant amount of technology and information to effectively coordinate forces and operations.
Coupled with the increased transparency of the confrontation environment, these factors severely limit the ability to conceal forces and conduct combat operations, requiring the identification of alternative solutions to achieve surprise of the adversary, but also to ensure the protection of one's own forces.

In addition, a mix of manned, unmanned and autonomous systems will bring a further shift in lethality and employability, while hypersonic, ballistic, long-range missile and space-based counter-operation capabilities will further extend the competitive domain. All these features of the current nature of armed conflict require us to rethink our own command and control systems in order to respond as effectively as possible to today's challenges.

In addition, the complexity and high dynamics of change in today's operational environment create entangled and hidden problems whose solutions are increasingly difficult to identify. Within this framework, the human side of C2 systems must

insist on the adoption and development **of a "red teaming" mentality** that ensures the development of critical and creative thinking among its own personnel (UK Ministry of Defence 2021, 1; JDP 0-01.1 2023, 50).

The commander remains a critical element of the command-and-control system, as the ongoing Russian-Ukrainian conflict demonstrates. The ability to inspire and motivate subordinates has proven to be a particular quality that has increased the resilience of the Ukrainian people, contributing to the morale component of combat capability. Leadership has been and will continue to be a defining element of conflict, with the potential to motivate and unite individuals and maintain the high operational capability of armed forces (MCDC 2020, 4). In addition, the same conflict demonstrated that the use of the concept of mission command was fundamental to achieving Ukrainian decision superiority over the Russians. Trusting subordinate commanders and giving them freedom of action to fulfil the intent of the higher echelon is the essence of mission command.

In addition, given Romania's position as a member of the North Atlantic Alliance, any military operations in which the Romanian military will participate will certainly be multinational. For this reason, the design of future C2 systems must take into account a crucial aspect of **multinational operations**, namely interoperability, in all its three dimensions: technical, procedural and human (AJP-01, 2022, 71).
The result of the analysis of the impact of the nature of the current conflicts on the command-and-control systems and the potential solutions to adapt them is shown in the next table.

2.3. Analysis of trends in the evolution of operating environment and their influence on C2 systems

Evolving trends in the operational environment are a critical factor in analysing how command and control systems adapt. In a context of rapid change and advanced technological developments, military structures must continuously adapt their C2 systems to meet new challenges. This adaptation involves not only the integration of new technologies but also the re-evaluation of decision-making processes in order to respond effectively to the complexity and dynamics of current and future conflicts.

To identify the influence of evolving trends in the operational environment on C2 systems, it is first necessary to understand what these trends are. We have therefore undertaken a comparative analysis of the evolutionary visions of three major actors in international relations who have recently published papers on the subject: the United States (TRADOC G2 2024), the United Kingdom (UK Ministry of Defence 2024) and NATO (NATO 2023).

All these analyses have one thing in common: technology. For the military, too, it plays a vital role in shaping the operating environment of the future. **New technologies** that combine processing power, connectivity, automation, quantum

TABLE NO. 2

Analysis of the impact of the current conflicts' character on command-and-control systems

Factor 2 – *Specific features of the character of current conflicts*	
Deductions	**Conclusions**
2.1. High transparency of the confrontation space due to the development of information collection systems	**2.1.1. Enhanced measures to protect C2 systems (ST, PC, Pe)** - development and deployment of network protection technology in cyberspace; - physical protection of command posts - dispersion, OPSEC measures, counter-drone systems (EW, AD systems, other types of weapons - e.g. lasers) etc. - training personnel on the use of OPSEC measures. **2.1.2. Advantages of situational understanding. (Pr, Pe)** - adjusting the JISR process to collect relevant data; - understanding the limitations of data collection systems in order not to fall into the trap of being misled (seeing is not synonymous with understanding).
2.2. Large volume of data due to the development of information collection systems	**2.2.1. The need to invest in emerging technology to increase collection capabilities and rapidly analyse large volumes of data. (ST, Pr, Pe)** - integration of Artificial Intelligence in support of specific processes of command-and-control systems; - technologizing collection systems to reduce their limitations (weather, electromagnetic spectrum, time - day/night) in an effort to ensure situational understanding; - it must be well understood what the role of the human factor will be and how much the decision should and can be automated. **2.2.2. Increased potential for errors due to inability to analyse relevant data (Pr, Pe)** - decision-making must necessarily include a risk management process; - training commanders and command staff in risk acceptance and risk management. **2.2.3. Increased chance of being misled (Pr)** - the inability to manage the large volume of data can contribute to misunderstanding the situation and create opportunities for the adversary to deceive us; - a process needs to be developed to counter misleading, with preparedness being an essential first element of this process.
2.3. Digitizing the battlefield	**2.3.1. Opportunities speeding up own decision-action cycle (Pr, Pe)** - implementation of artificial intelligence systems and analysis algorithms to manage the large volume of data; - developing mechanisms to prioritize information essential for decision-making in a short timeframe; - training staff to optimize the interpretation and use of digital information. **2.3.2. The need for advanced cyber security measures and protection against interference. (Pr, Pe, ST)** - implementation of a continuous monitoring and defence system against cyber-attacks; - Integrating redundancy and business continuity measures in case of cyber-attacks; - increasing resilience by training staff on cyber risks and security measures.
2.4. The operating environment is highly contested	**2.4.1. Creating more agile command structures capable of operating in contested environments. (PC, Pe, ST)** - optimizing communication networks for mobility and increased security; - adopting dispersed command post practices and using redundant systems; - training staff to operate in analogue mode as well; - introducing additional security measures to protect C2 sites against direct and indirect attacks (e.g. drones). **2.4.2. Implement passive and active safeguards to reduce footprinting and masking of command posts (ST, PC, Pe)** - development and use of equipment and technologies to reduce the thermal and electromagnetic footprint, including multi-spectral electromagnetic shielding and cloaking systems; - optimization of C2 architecture to allow modular and flexible configuration, reducing visibility and time required for installation/deployment in the field; - increased pre-emptive detection capabilities, identifying any adversary surveillance threat early.
	2.4.3. Increased mobility to avoid detection and attacks (Pe, Pr, PC) - introducing mobile command posts and small C2 equipment that can be quickly transported and installed in new locations. - the adoption of rapid relocation procedures to increase the difficulty of detection and tracking by the adversary. - train personnel to operate in high mobility scenarios, preparing rapid procedures and processes for disconnecting and reconnecting to communications and data networks.

Deductions	Conclusions
2.5. The multidimensionality of confrontation	**2.5.1. Development of integrated and interoperable C2 structures (ST, PC, Pr, Pe)** - implementing multi-domain C2 architectures capable of simultaneously managing operations in land, air, maritime, cyber and space; - creating secure and fast communication channels among domains to enable the exchange of relevant information in real-time; - training C2 personnel to understand the specificities of each domain of operation. **2.5.2. Increased capacity to process and analyse data from different domains (ST, Pr, Pe)** - using artificial intelligence and advanced algorithms to integrate data from multiple domains, providing a coherent operational picture; - creating a system for automatically prioritizing information so that critical data from any domain is quickly flagged to decision-makers; - optimizing cross-domain coordination processes to ensure that actions in any operational space are synchronized and support overall mission objectives. **2.5.3. Flexibility and adaptability of C2 structures for efficient and coherent response in several areas (ST, PC, Pr)** - development of configurable C2 procedures and equipment to allow rapid adaptation to the specific requirements of each domain; - introduction of scalable command and control modules to enable effective responses at different levels of intensity and in a variety of operating environments; - ongoing training of personnel in adapting and coordinating responses to interdependent operations in multiple domains, thereby increasing operational resilience.
2.6. Multinational operations	**2.6.1. The need to achieve interoperability between C2 systems (ST, PC, Pr, Pe)** - adoption of common communication and security standards to enable connectivity between different C2 systems, facilitating information exchange and operational coordination; - development of standardized protocols and common formats for reporting and transmission of orders, which are user-friendly for all forces involved; - the implementation of interoperability programs to familiarize partner forces with allied equipment and procedures, thereby increasing operational cohesion. **2.6.2. Investment in staff training and joint training for multinational operations (PC, Pr, Pe)** - organizing regular multinational exercises to train C2 personnel from allied forces in working together; - creating common training manuals and procedures, including practices and protocols for rapid coordination in multi-nation operating contexts; - encouraging the exchange of personnel and experience between partner nations, thereby increasing mutual understanding and integrated responsiveness. **2.6.3. Developing a communications infrastructure tailored for multinational operations (ST, PC)** - ensuring deployment of interoperable, secure and efficient communications networks that support the rapid exchange of information between allied forces without security vulnerabilities; - investing in portable communications technologies and equipment compatible with partner forces' networks so that information is available to all parties involved.

computing, machine learning and artificial intelligence will enable not only a new generation of weapon systems but also new ways of waging war.

All of this has a direct impact on military-specific C2 systems. Innovative technologies can help to speed up the decision-making process by processing and analysing large amounts of data, providing the basis for a near-complete operational picture at all levels of conflict. The main benefits of integrating emerging technologies into C2 systems are recognized to include (NIAG 2022, 1-29 - 1-30):

- faster and deeper understanding of the operational situation
- faster targeting of forces relative to the enemy;
- increased synchronization of operational effects on the battlefield;
- improved processes, capabilities and effects realized through other

combat functions such as logistic support, protection, fire support or intelligence activities.

In support of command and control, technology has the practical ability to improve:

- the collection, analysis, fusion, sharing and, most importantly, exploitation of data from all relevant sources for all relevant domains to provide the best possible situational understanding and thus ensure the information advantage on the battlefield;
- the effective use of this information to make better-informed and better-calculated decisions, thereby ensuring decision advantage over the adversary;
- the synchronization of information and effects of operations across environments and theatres;
- the optimization of the tempo of battle to achieve superior enemy decision tempo.

Considering the increasing dynamics and growing complexity of military confrontations, it is expected that technology will be a primary factor in building new C2 systems. The analysis and impact of the main emerging technologies with relevance in this respect are presented in the table below (NIAG 2022, 3-106 - 1-115; NATO Science & Technology Organization 2020, 41 - 111).

TABLE NO. 3

Analysis of the impact of the main emerging technologies in the construction of new C2 systems

Technology	Details	How can it support the C2
Artificial intelligence	• Artificial intelligence (AI) is the ability of machines to perform tasks that typically require human intelligence. These tasks include recognizing patterns, learning from experience, drawing conclusions, making predictions, and making decisions or initiating actions. • AI mimics aspects of human cognition such as perception, reasoning, planning, and learning. This technology can autonomously perform tasks such as planning, understanding language, recognizing objects and sounds, learning, or solving problems. • It is considered by many experts to have the most revolutionary impact on society in general and military systems in particular. • Russian President. Vladimir Putin, estimated in 2017 that "artificial intelligence is the future... Whoever becomes a leader in this field will rule the world." (Russia Today 2017). • One advantage is that it is not influenced by factors such as stress or fatigue. (Dragomir and Alexandrescu 2017, 58)	- data analysis; - improving data collection capabilities; - developing strike systems and their effects; - performing specific tasks at command posts; - increasing disinformation capabilities (e.g., deepfake); - supporting the operational planning process by providing faster and more efficient methods for comparing and analyzing courses of action (war gaming).
Blockchain	• Blockchain is a distributed ledger technology that combines elements of cryptography, consensus, and distributed systems. It enables decentralized and secure data storage through a structure of linked blocks of information that are shared, replicated and synchronized among network members. • Blockchain ensures high data security by making it impossible to change an existing block without changing all subsequent blocks. The technology thus prevents retroactive alteration of data and ensures information integrity. • In a military context, blockchain offers the potential for coherent data exchange between different hierarchical structures, such as sensor networks or command posts. It enables a secure and synchronized flow of information in distributed and complex environments.	- increasing data exchange; - ensuring situational understanding; - ensuring data and communication security.

Technology	Details	How can it support the C2
Human Augmentation	• Human augmentation refers to technologies used to enhance human performance. In the military context, it includes human physiological, social, and cognitive domains, as well as advanced human-machine interfaces. • Major categories of human performance enhancement include: - Enhanced/extended senses (e.g., augmented vision, hearing, taste, smell) that add new informational dimensions to C2 systems. - Enhanced cognition, achieved by identifying the human cognitive state and tailoring computerized feedback to the user's needs, thereby accelerating decision-making. - Augmented action, achieved by monitoring human actions and mapping them to local, remote, or virtual environments.	- increase situational understanding; - increase the efficiency of human data analysis and processing; - improve the speed at which people work; - revolutionize the way people share information; - improve decision-making by limiting the influence of cognitive biases.
Internet of Battle Things (IoBT)	• The basic idea of IoBT is to connect all elements available on the battlefield (vehicles, drones, soldiers, wearables, weapons, sensors, etc.) into a self-configuring network to facilitate the exchange of information. For example, the health status of soldiers can be shared via a monitoring system, images captured by a weapon's camera can be shared with intelligence structures at the command post, or video from a UAV, aircraft, or satellite can be transmitted to a reconnaissance patrol in the area.	- easy exchange of information; - supporting situation monitoring; - providing situational understanding; - supporting Battle Damage Assessment (BDA)
5G / 6G/ 7G Technology	• Cellular technology is used not only to connect people with handheld devices (e.g. smartphones) but also to connect almost all types of devices (computers, sensors, etc.). 5G technology will be available in the next 10 years, while 6G, currently in the definition phase, could be fully available by 2035, according to estimates, offering greater coverage, higher transmission speeds, centimetre-level location accuracy and edge computing. By 2040, 7G could be in the planning stages. Both technologies enable network slicing, which facilitates the deployment of "private" networks using commercial off-the-shelf equipment and commercial networks.	- securing transmitted data; - increasing situational understanding.
Quantum Technology	• Quantum technologies will play an important role in improving situational awareness, communications and cybersecurity capabilities. The categories into which quantum technologies can be divided in the C2 context are: sensing, communications, and computing. The major achievements in each category by 2040 could be: - Sensing: quantum sensors for C2 applications, portable quantum navigation devices. - Communications: Point-to-point secure quantum links, secure Internet for defence, the combination of quantum and classical communications. - Computing: Quantum computers will outperform classical computers.	- enhancing situational understanding; - ensuring cyber security.
Hyper-automation (robotization)	• To excel in automation, the combination of multiple technologies can help create smart spaces - physical environments in various domains where people and technology enable systems to interact, connect and coordinate, seeking to minimize human intervention and optimize effort. • Hyper-automation is expected to reach a profound level of expansion by 2040, with digital processes becoming an essential part of any military operation, including robotic process automation to reduce human intervention (especially in repetitive tasks) and AI-driven decision-making at all stages of OODA. Human intervention will be focused only on high-value activities in planning and tasking, as well as on key decisions (human-in-the-loop).	- reorganization of force structures; - reconfiguring how orders are transmitted; - increasing the efficiency of operational processes; - increasing lethality; - human-robot interoperability; - rapid decision making.

Although we are witnessing an unprecedented rephonologization of society, we believe that **decision-making will remain a human attribute**, at least for the foreseeable future. This statement is supported by the increasing uncertainty of the operational environment, but also by the fact that the way the brain works is prone to

systemic errors and biases (AJP3.10.2 2020, 42); thus, future C2 systems will have to adapt, with the commander still at the centre of the operational process. This means that they must be adequately trained and educated to effectively perform the specific functions of directing the entire military operation. Commanders must develop the ability to accurately understand the operational environment, visualize solutions to operational problems, effectively communicate those solutions to subordinates, direct execution in response to volatile and dynamic battlefield conditions, provide command and control of forces, and continuously assess progress to ensure timely adaptation to the challenges of the operational environment. In addition, commanders' training must include a component of internal reflection on their own cognitive limitations that may affect the quality of decision-making.

The rationale for including such an educational component is demonstrated by the flawed planning assumptions made by the Russians at the outset of the conflict, and the incalculable consequences of such decisions based on flawed prejudices. What was supposed to be a three-day special operation (Watling and Reynolds 2022, 1) turned into a nearly three-year conflict for the Russians, in which considerable resources and effort were invested.

Conclusions and proposals

In the information age, while some aspects of command and control (C2) remain unchanged, such as the nature of warfare, uncertainty and time pressure, technological developments have brought about fundamental changes. Today's world is characterized by instability and rapid change, and these characteristics are reflected in the military context. In such an era, C2 systems must be highly adaptable and perform effectively, regardless of the type of conflict or environment in which they operate. Technology has a critical role to play in enhancing C2 capabilities, but it also poses significant risks. On the one hand, technology can help to optimize decisions and make coordination more effective, but on the other hand, there is a risk of over-reliance on equipment and information overload. This can create a dangerous illusion that war can be fought with absolute precision, which is not realistic. In addition, as C2 systems become more sophisticated and interconnected, the risks of disruption, cyber-attack or information overload increase. Solutions must therefore be found to protect and optimize the data flows specific to command-and-control systems. Increasing the resources devoted to research and innovation in emerging technologies to ensure a competitive edge over adversaries can ensure breakthroughs that support more efficient C2 systems.

However, this article was not intended to be a roadmap for the adaptation of command-and-control systems, but it was rather meant to highlight some extremely important elements to be considered in the implementation of the transformation plan. The analysis of the immutable characteristics of the nature of conflicts, as

well as those of the current ones, and the trends in the evolution of the operational environment were the pillars on which we built the results presented.

Although we understand that the process of transforming the Romanian command and control system should not be an individual effort, but rather a collective one, well directed by the decision-makers at the highest level of the Romanian Army, we believe that this article can support this endeavour through at least two **extremely valuable elements**:

- the results obtained, which can be used as a basis for adapting C2 systems;
- the scientific way in which we have developed these results. Identifying, in the first phase, the factors that can influence C2 systems and how they can do so, and then, through a process of inference, determining how to adapt them, is what we consider to be the right approach for the transformation of command-and-control systems in the Romanian Army.

In the following lines, we will present **the main results of the scientific approach** undertaken, in the form of recommendations for the main target of this study, the decision-makers of the Romanian Army, organized by the four components of the command-and-control systems highlighted in the first section of this paper. These results emerged from a thematic analysis of the data derived from applying the "three-column factor analysis" method in the previous section. All the resulting data were subjected, at this stage, to a rigorous analysis process aimed at organizing them into broader themes, which were subsequently classified into the four major categories of command-and-control systems, according to the specific characteristics of each.

Personnel

- The commander will continue to be at the centre of the decision-making process. This requires continuous training. In addition, creating a system for transferring institutional memory from one generation to the next, from one commander to future commanders, can make training more effective.
- Leadership must remain the fundamental element of military command.
- The need to adopt a "red teaming" mentality to ensure the development of critical and creative thinking in one's own staff.
- The development of critical and creative thinking focused on producing effects that slow down the enemy's decision-action cycle.
- The need to train personnel to operate digital systems amidst the technologization of command-and-control systems.
- Training personnel to operate in analogue mode, given the increased possibility of operating in a contested environment against an adversary with enhanced electronic warfare capabilities.
- Staff training should focus on *how* to think, rather than *what* to think. Such an approach can provide staff with the necessary mental flexibility to adapt and respond effectively to the challenges that may arise in the increasingly volatile and uncertain operating environment.

- Understanding how the human brain works in decision-making and the errors in judgment that can occur as a result of one's own cognitive biases.
- Implementation and training of the Mission Command concept must begin in peacetime. If it is not implemented in day-to-day operations, it is unlikely to be effective in war.
- The need to achieve human interoperability between own and allied C2 systems in the context of the increasing likelihood of military operations in multinational environments.

Processes
- Adapting unit battle tempo to reduce decision time by incorporating new technologies.
- Shorten your own decision-action process.
- Optimize operational processes through the use of emerging technologies.
- Ability to communicate the full operational picture to the lowest echelons in real time and automatically update it at all levels of command.
- Reducing the size of transmitted orders or using emerging technologies to ensure rapid understanding. For example, NATO corps-level operational orders routinely run to 750 pages and joint-level orders to a thousand pages. Few people in a command read them in their entirety (Storr 2023, 87).
- The need to achieve procedural interoperability between national and allied C2 systems as the likelihood of conducting military operations in multinational environments increases.

Technological systems
- The digital transformation of command centres by integrating new technologies to support the rationalization of processes specific to the functions of command and staff systems (situational awareness, decision-making, etc.).
- The use of high-performance technological systems to facilitate the rapid generation, transmission, reading and understanding of written orders. This can reduce the planning time for new operations, with a direct impact on reducing the OODA cycle.
- The need to identify technical solutions to protect C2 systems: reducing cyber, electromagnetic and thermal footprints, etc.
- Dependence on technology can also create vulnerabilities in a contested environment and in the face of an adversary with enhanced electronic warfare capabilities.
- The need to achieve technical interoperability between one's own and allied C2 systems, given the increased likelihood of conducting military operations in a multinational environment.

Command posts
- Provide increased protection: physical and electromagnetic.
- Rethink the way command posts are organized (their current size is far too large

and they are far too static, making them extremely vulnerable in an era of increased remote weapon accuracy and reduced time between detection and engagement to minutes) to meet the increasing challenges of the operational environment and to ensure their survivability and continued C2 functionality (e.g. adopting command post dispersion practices and using redundant systems. Integrated and functional modules may no longer need to operate from the same location, and when we talk about the Basic Command Post, we no longer mean a single location, but a variety of locations/modules that together, with technology support, fulfil the functions of that command point).
- Implement additional security measures to physically and electromagnetically protect C2 sites from direct and indirect attack (e.g. from drones or enemy EW systems).
- Reduce and mask the size, thermal and electromagnetic footprint of command posts. (e.g. investing in silent batteries to allow PC-based technical systems to run for as long as possible, replacing noisy generators and identifying solutions to replace noisy air conditioning systems that can give away the location of command posts). "The war between Russia and Ukraine makes it clear that the electromagnetic signature emitted by command posts over the past 20 years cannot survive against the speed and precision of an adversary with sensor-based technologies, electronic warfare, unmanned aerial systems or access to satellite imagery." (Nagl 2024, 24)
- The use of measures to mislead the adversary by creating false command posts can be a solution in the effort to increase the protection of C2 systems (Nagl 2024, 242).
- Increase command post mobility to avoid detection and attack. The constant movement of PCs to avoid detection with continuous realization of C2 functionality.
- The need to achieve interoperability between own and allied C2 systems, given the increased likelihood of conducting military operations in a multinational environment.

Furthermore, the principles that must underpin new command and control systems, in order to ensure a high degree of adaptability to the current and future operating environment challenges, are flexibility, modularity, survivability, small footprint and resilience.

Flexibility implies the ability of the command and control (C2) system to adapt rapidly to changes in the operational environment. This principle includes both adaptable structures and procedures and the use of technology to enable rapid responses to unforeseen challenges. The flexibility of the C2 system is essential to respond quickly to new threats or opportunities and to adjust priorities and resources as the battlefield evolves.

Modularity means building the system from independent but interoperable components that can be combined and reconfigured as required. In the C2 context, this principle allows the creation of tailor-made structures for each mission and facilitates modernization by integrating new technologies without affecting the

whole system. Modularity enables armed forces to optimize resources and improve operational efficiency.

Survivability refers to the ability of the C2 system to operate under adverse conditions, including contested environments. This principle can be achieved through appropriate dispersion, small size, redundancy, mobility, manoeuvrability, camouflage, deception, OPSEC measures, and the integration of anti-drone systems and other defensive technologies to provide adequate physical and cyber protection. The goal is to reduce vulnerability to enemy attack and ensure continuity of operations.

Reducing the ground footprint means minimizing the physical size and electromagnetic signature of command posts, thereby reducing the chances of being detected and hit by the enemy. (One solution may be to disperse and conduct operations from multiple remote locations that operate as a whole.) A reduced-footprint C2 system is more difficult to identify and locate, contributing to the safety of personnel and equipment. This principle is essential against adversaries with advanced surveillance and attack capabilities.

Resilience refers to the ability of the system to recover quickly from a disruption or attack and maintain long-term functionality. Resilience includes system redundancy, backup procedures, and continuity plans to enable operations in the event of loss or disruption. This principle ensures that in the face of attack or failure, C2 systems can continue to perform their essential mission without compromising the overall effectiveness of operations.

To summarize, adapting command and control systems to meet the challenges of today's operational environment requires a holistic and integrated approach that takes into account both technological evolution and changes in global conflict dynamics and evolving trends in the operational environment. In this regard, C2 systems must strike a balance between the use of technology and human adaptability. It is also crucial to develop and implement flexible strategies that allow for rapid adaptation to unforeseen changes, as well as mandatory testing in different contexts of potential adaptive solutions for command-and-control systems. This will ensure coherent and flexible operations, which are essential in the face of the complex and dynamic challenges of modern warfare.

References

ADP 6-0. 2019. *Mission Command: Command and Control of Army Forces.* Washington DC: US Headquarters Department of the Army.

AJP-01. 2022. *Allied Joint Doctrine, Edition F, Version 1.* NATO Standardization Office.

AJP-3. 2019. *Allied Joint Doctrine for the conduct of operations.* C, Version 1. NATO Standardization Office.

AJP3.10.2. 2020. *Allied Joint Doctrine for operations security and deception, edition A, version 2* . NATO Standardization Office.

AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations, edition B, version 1.* NATO Standardization office.

ATP 3.2.2. 2016. *Command and Control of Allied Land Forces.* B, Version 1. NATO Standardization Office.

Bailey, Kathryn. 2023. *Army looks to transform future command and control.* https://www.army.mil/article/267509/army_looks_to_transform_future_command_and_control.

Beagle, Lt. Gen. Milford "Beags", Brig. Gen. Jason C. Slider, and Lt. Col. Matthew R. Arrol. 2023. „The Graveyard of Command Posts." *The Military Review* 10-24. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2023/Graveyard-of-Command-Posts/.

Collins, Major General Charles. 2023. "Mobilizing the British Army." *The British Army Review* (182): 6-9.

Creswell, John W., and J. David Creswell. 2023. *Research design. Qualitative, Quantitative, and Mixed Methods Approaches, ediția a șasea.* Los Angeles: Sage Publications.

Crilly, Martin, and Alan Mears. 2022. *Multi Dimensional and Domain Operations (MDDO).* https://wavellroom.com/2022/01/26/mddo/.

Dragomir, Florentina-Loredana, and Gelu Alexandrescu. 2017. "Aplicații ale inteligenței artificiale în fundamentarea deciziei." *Buletinul Universității Naționale de Apărare „Carol I"* 56-61.

Ellison, Davis, and Tim Sweijs. 2023. *Breaking Patterns Multi-Domain Operations and Contemporary Warfare.* Hague: The Hague Centre for Strategic Studies.

Gosselin-Malo, Elisabeth. 2024. *Drone warfare in Ukraine prompts fresh thinking in helicopter tactics.* https://www.defensenews.com/global/europe/2024/07/19/drone-warfare-in-ukraine-prompts-fresh-thinking-in-helicopter-tactics/.

Hambling, David. 2020. *The 'Magic Bullet' Drones Behind Azerbaijan's Victory Over Armenia.* https://www.forbes.com/sites/davidhambling/2020/11/10/the-magic-bullet-drones-behind--azerbaijans-victory-over-armenia/.

JCN1/17. 2017. *Joint Concept Note (JCN) 1/17 Future Force Concept.* UK Ministry of Defence.

JDP 0-01.1. 2023. *Joint Doctrine Publication 0-01.1 UK Terminology Supplement to NATOTerm.* Edition B. UK Ministry of Defence.

JP-1. 2017. *Joint Publication 1 Doctrine for the Armed Forces of the United States.* US Joint Chiefs of Staff.

Leavy, Patricia. 2023. *Research Design - Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches, ediția a doua.* New York: The Guilford Press.

Multinational Capability Development Campaign [MCDC]. 2020. *Future Leadership.* https://assets.publishing.service.gov.uk/media/5fdccd0de90e07452ec36ee8/20201210-MCDC_Future_Leadership-web.pdf.

MCDP-6. 2018. *Command and Control.* US Marines Corps.

Molloy, Dr Oleksandra. 2024. *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine.* Australian Army Research Centre.

Nagl, John A. 2024. *A call to arms: Lessons from Ukraine for the Future Force.* Strategic Studies Institute, UIS Army War College.

NATO. 2022. *Initial Alliance Concept for Multi-Domain Operations.* Norfolk: NATO Allied Command Transformation.

__. 2023. *Strategic Foresight Analysis 2023.* Norfolk: NATO Allied Command Transformation.

NATO Industrial Advisory Group [NIAG]. 2022. *Command and Control Capabilities in support of Multi Domain Operations (Multi Domain C2).*

NATO Parliamentary Assembly. 2022. *The future of Warfare.* NATO Science and Technology Committee.

NATO Science & Technology Organization. 2020. *Science & Technology Trends 2020-2040 - Exploring the S&T Edge.* Bruxelles. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

Nilsson, Niklas. 2023. "Commanding Contemporary and Future Land Operations." In *Advanced Land Warfare. Tactics and Operations*, by Mikael Weissmann and Niklas Nilsson, 43-62. Oxford University Press.

Russia Today. 2017. https://www.rt.com/news/401731-ai-rule-world-putin/.

Stanciu, Cristian-Octavian, and Silviu-Iulian Gimiga. 2023. "Noile tehnologii și impactul lor asupra domeniului militar." *Buletinul Universității Naționale de Apărare „carol I"* 12 (2): 157-169.

Storr, Jim. 2023. "The Command of Land Forces." In *Advanced Land Warfare. Tactics and Operations*, by Niklas Nilsson Mikael Weissmann, 87-103. Oxford University Press.

TC 7-102. 2014. *Training Circular No. 7-102 Operational Environment and Army learning.* Washington DC: Headquarters Department of the Army.

The International Institute for Strategic Studies [IISS]. 2023. *Strategic Survey 2022. The Annual Assessment of Geopolitics.* Londra, Routledge.

TRADOC G2. 2024. *The Operational Environment 2024-2034: Large-Scale Combat Operations.* US Army Training and Doctrine.

UK Ministry of Defence. 2024. *Global Strategic Trends: Out to 2055.*

—. 2020. *Introducing the Integrated Operating Concept 2025.*

—. 2021. *Red Teaming Handbook.* 3rd. https://assets.publishing.service.gov.uk/media/61702155e90e07197867eb93/20210625-Red_Teaming_Handbook.pdf.

Wade, Norman M. 2023. *AODS 7 The Army Operations & Doctrine Smartbook - Multidomain operations.* The Lightning Press.

Watling, Jack, and Nick Reynolds. 2022. *Operation Z. The Death Throes of an Imperial Delusion.* Royal United Services Institute for Defence and Security Studies.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The role of civil-military cooperation in contemporary United Nations peacekeeping operations: a case study of UNIFIL

Assist. Prof. Slobodan M. RADOJEVIC, Ph.D.*

*University of Defense, Military Academy, Belgrade, Serbia
e-mail: slobodan.radojevic@va.mod.gov.rs

Abstract

The paper explores the place and role of civil-military cooperation (CIMIC) in contemporary United Nations (UN) peacekeeping operations. The author's starting point is that civil-military cooperation is important for the success of a peacekeeping operation, as the CIMIC personnel engage in the implementation of CIMIC tasks in order to create a favorable civilian environment. Through these activities, the CIMIC personnel influence the security of the unit and contribute to the success of the mission. The paper aims to advance the understanding of civil-military cooperation by clarifying how the concept is understood, shaped, and applied in contemporary UN peacekeeping operations. With this in mind, the interview has proven to be the best research technique for obtaining information on how the CIMIC personnel understand, implement, and develop the functions of the CIMIC in UN peacekeeping operations. This section presents experiences in the application of the CIMIC in the peacekeeping operation in Lebanon (United Nations Interim Force in Lebanon – UNIFIL) as a case study. The paper emphasizes that the successful implementation of civil-military cooperation in a peacekeeping operation can affect the strategic level, i.e. exert an influence on the success of the operation itself. Emphasis is placed on presenting the range of roles and functions that the CIMIC personnel perform in peacekeeping operations under the auspices of the UN. The paper concludes that contemporary peacekeeping operations have evolved and require a significant component of civil-military cooperation.

Keywords:

civil-military cooperation (CIMIC); CIMIC personnel; peacekeeping operations; civil environment; United Nations; UNIFIL.

Article info

Received: 5 November 2024; Revised: 27 November 2024; Accepted: 6 December 2024; Available online: 17 January 2025

Citation: Radojevic, S.M. 2024. "The role of civil-military cooperation in contemporary United Nations peacekeeping operations: a case study of UNIFIL". *Bulletin of "Carol I" National Defence University*, 13(4): 113-125. https://doi.org/10.53477/2284-9378-24-52

Civil-military cooperation had been found long before it was officially established. During World War II, General Dwight D. Eisenhower realized: "The sooner I can get rid of all these questions that are outside the military in scope, the happier I will be! Sometimes I think I live ten years each week, of which at least nine are absorbed in political and economic matters." (Eisenhower 1942). Modern, defined and precisely determined civil-military cooperation (CIMIC COE 2022a) is a consequence of changes that have affected all the armies of the world through the evolution of conflicts, the conditions of warfare themselves, but also the use of the army. Encountering the problems of using armed forces, primarily outside one's own territory, and the limitations in the response of military units in situations related to the civilian population, the need arose to form a special military function that would understand the non-military component in the area of operation and establish communication and cooperation with all factors surrounding military units. Through use in different environments, within different operations and missions, civil-military cooperation has evolved and developed into the form that we encounter today in the modern armed forces of the world.

The paper aims to present the role of CIMIC in contemporary United Nations peacekeeping operations. The paper therefore discusses civil-military cooperation as defined in United Nations strategies and documents. This approach was chosen because the aim of the paper is to present the role of civil-military cooperation in contemporary peacekeeping operations under the auspices of the United Nations, with a focus on examining practices and experiences from operations in which members of the Serbian Armed Forces participated.

Civil-military cooperation

In the most general sense, civil-military cooperation represents the coordination and cooperation of the military and the civilian environment in the area of operation, in order to support the mission and tasks of the military unit. The importance of civil-military cooperation lies in establishing key links between military and civilian actors, at a certain level and space, in order to contribute to the achievement of primarily military, and then common interests through mutual activities. The decisive goal of civil-military cooperation, from a military perspective, is the establishment of a safe and secure environment and the increase of trust between the military and civilians. It involves communication and joint action of civilian and military entities through the political, security, humanitarian, development, and other dimensions of military operations in order to achieve goals related to conflict prevention, building, strengthening, and maintaining peace, as well as creating conditions for the provision of humanitarian assistance.

The factors of the civil environment are: the population, authorities, business entities, international organizations, non-governmental organizations, religious

organizations and movements, etc. In an international environment, characterized by the presence of different communities, a good assessment of the civil environment is vital, which refers to the observation of different characteristics and influences. Ignorance of the authorities, the state of the economy, the presence of international and non-governmental organizations, the composition of the population, as well as religious beliefs, customs, and traditions of the population in the civilian environment in which a military unit is engaged can have a negative impact on the success of the mission. CIMIC personnel are responsible for familiarizing military forces with the specifics of the factors of the civil environment in the area of operation, and the principle of impartiality and neutrality is the basis for the successful implementation of tasks.

It is important to emphasize that the CIMIC personnel must understand the commanders' intent and plan and propose CIMIC activities, in accordance with a well-founded, high-quality, but also timely assessment of the factors of the civilian environment that affect the execution of the unit's mission. In fact, CIMIC personnel are engaged in peacekeeping operations to implement CIMIC tasks in order to create a favorable civilian environment. Their activities, i.e. the proper and efficient application of CIMIC, increase the security of the unit and contribute to the success of the mission. The use of CIMIC in peacekeeping operations requires good training of the engaged forces and full knowledge and compliance with CIMIC procedures that are applied in contemporary peacekeeping operations and in a complex environment.

Furthermore, in addition to CIMIC as a military function, we will look at CIMIC in the UN, which implies CIMIC as cooperation between the military and civilian components of the UN mission and the UN Civil-Military Coordination, i.e. cooperation between UN mission personnel and humanitarian organizations. Civil-Military Coordination (CMCoord) in the UN system "is the system of interaction, involving the exchange of information, negotiation, de-confliction, mutual support, and planning at all levels between military elements and humanitarian organizations, development organizations, or the local civilian population, to achieve respective objectives." (UN DPKO 2002, 2-3).

The definitions of CIMIC used by NATO are somewhat different, although their essence is the same. Namely, in 2022 NATO approved the new definition for CIMIC as: "a military joint function that integrates the understanding of the civil factors of the operating environment and that enables, facilitates and conducts Civil-Military Interaction (CMI) to support the accomplishment of missions and military strategic objectives in peacetime, crisis and conflict" (CIMIC COE 2022).

Also, from 2022 new definition for CMI is: "activities between NATO military bodies and non-military actors to foster mutual understanding that enhances effectiveness and efficiency in crisis management and conflict prevention and resolution"

(CIMIC COE 2022a). CIMIC is a cross-functional facilitator of CMI, using the liaison structure to facilitate the coordination mechanism. NATO CIMIC Core functions are: Civil-Military Liaison; Support to the Force and Support to the Civil Actors and their Environment (NATO CIMIC & US Civil Affairs Doctrinal Review & Comparative Assessment 2022, 11-12; Garbino, Robinson and Valdetaro 2024). Namely, in addition to the above, in the field of CIMIC, there are developed policies, strategies, and doctrines of the European Union, African Union, and others which will not be discussed further, as the subject of the work is exclusively UN peacekeeping missions.

Contemporary UN Peacekeeping operations

After the end of the Cold War, due to the increase in the number, intensity and nature of conflicts in the world, the UN has significantly increased the number and capacity of peacekeeping forces, and civil-military cooperation has become increasingly important. Actually: "the end of the Cold War marked the emergence of new conflicts on the global stage and implicitly an increased number of UN missions" (Manga 2023, 174). Traditional peacekeeping operations with a small number of civilian participants have been replaced by contemporary peacekeeping operations with an increased number of civilian components in the area of operation. At the same time, the capabilities of military units for civil-military cooperation have increased due to the increasing involvement of military units in peacebuilding operations and the provision of humanitarian assistance in vulnerable areas. Therefore, in modern peacekeeping operations, military forces are engaged in multidimensional and complex environments, which imposes a comprehensive view of the influence of all relevant participants, and the success of a military mission is closely linked to the mutual relationship between military forces and civilian actors.

Over the years, peacekeeping has evolved from a primarily military model of observing ceasefires and separating forces after wars and conflicts, to a complex model composed of many elements, military, police, and civilians, working together to help countries affected by wars and conflicts create the conditions for sustainable and lasting peace.

Peacekeeping operations are: "one of the instruments for resolving crises in the world and preventing armed conflicts that threaten global peace and security" (Radojević and Blagojević 2024, 141). Today's multidimensional peacekeeping operations serve not only to maintain peace and security but also to facilitate the political process; protect civilians; assist in the demining of territory; in the disarmament, demobilization, and reintegration of former combatants; support the organization of elections; facilitate the transition from interim to transitional and ultimately to democratically elected governments; participate in the training and restructuring of new police forces; promote social and economic recovery and development;

facilitate the safe return or resettlement of internally displaced persons and refugees; protect and promote human rights and assist in the restoration of the rule of law, etc. (Langholtz, 2010; UN Peacekeeping 2024).
It is clear that a dynamic and innovative approach is something that characterizes modern peacekeeping UN operations. Coordination of all actors involved has a critical function in a complex peacebuilding operation and can be understood as an effort to ensure that the peace, security, and development dimensions of the peacebuilding operation are directed towards a common goal (De Coning 2005).

Specificity of civil-military cooperation in the UN peacekeeping operations

The research included an analysis of foreign experiences in the implementation of key CIMIC functions in UN peacekeeping operations, which in methodological and substantive terms shaped and guided this research (Parepa 2013; Guezen 2018; Esler 2020; Wassay and Butt 2022; De Araujo Grigoli 2022).
In contemporary peacekeeping operations, civil-military cooperation is particularly important and implies active coordination and cooperation between the military and civilian elements in the operation zone. Namely, military forces deployed to peacekeeping missions are trained and equipped to carry out the mission mandate and create a safe and secure environment for stabilizing the situation and building sustainable peace. On the other hand, in peacekeeping operations, the requirements for humanitarian assistance, police work, infrastructure reconstruction, and population reconciliation are beyond the military's purview and capabilities.

UN peacekeeping operations are often mandated to perform a wide range of functions. Creating a secure and stable environment is primarily a military function while supporting the political process and long-term social stability (including the rule of law, humanitarian assistance, development, etc.) are civilian functions. In this context, the basic principles of CIMIC in the UN are to facilitate the integration of efforts; to provide a key link with the civilian components of the peacekeeping operation and partners such as humanitarian and development actors, the host country's military and the local population; and to provide analysis related to military operations and support the implementation of the mission's mandate.

The military component of UN peacebuilding operations uses the UN Civil-Military Coordination (UN–CIMIC) branch to facilitate liaison and coordination with the civilian components of the mission, with the rest of the UN system, and with all other actors in their area of responsibility.
UN CIMIC personnel must develop a comprehensive civilian operational "picture" and analysis of it, in order to support the planning and conduct of military operations in the mission. It provides a link between the UN military, UN police, civilian components, host country authorities, United Nations agencies, funds and

programs, other international organizations, and international and national non-governmental organizations (UN DPKO 2022).

In fact, UN CIMIC is one element in a broader coordination network that contributes to general or systemic cooperation. Civil-military cooperation, within its rightful place at the operational and tactical levels in the context of UN peacekeeping operations, has a significant role in managing civil-military relations.

Most existing UN policies and guidelines are limited to civil-military cooperation focused on resolving humanitarian issues. UN CIMIC activities can have a beneficial impact on the overall peacebuilding process if "resources, energy, and goodwill can be positively channeled in support of the overall mission objectives and so that their UN CIMIC activities become complementary to the work undertaken by the humanitarian and development community" (De Coning 2005, 111).

Namely, the role of CIMIC is determined by the type and stage of the mission and should allow for flexibility. Lloyd and van Dyk emphasize the need for flexible CIMIC personnel to operate in a "participative and consultative management environment" (Lloyd and van Dyk 2007, 87). The CIMIC officers „need to understand the complexities between functioning in a cooperative versus a coexistent framework" (Lloyd and van Dyk 2007, 87). Lloyd and van Dyk summarize the roles and functions of the CIMIC officer as: adviser to the military commander; adviser to the humanitarian coordinator; coordination officer; project officer for community support initiatives; and training coordinator (Lloyd and van Dyk 2007, 87-89).

Civil-military cooperation is often misinterpreted as a tactical activity with a public relations agenda (Holshek and de Coning 2017), when in fact it is much more than that. UN CIMIC personnel undertake two core activities: "liaison and information exchange" and "assistance to civilians". The first core task of liaison and information exchange means that UN CIMIC personnel are the first point of "entry" for other actors in the civilian environment. In effect, they ensure that the military component is aware of the advantages and sensitivities of working with police components, civilian partners within the mission, and humanitarian organizations. CIMIC also ensures a transparent flow of information between military and civilian partners. The liaison function is carried out to support the management of civil-military interaction with the aim of assisting the military component commander in his efforts to implement the overall mandate of the mission. The aim is to ensure that the military component has adequate understanding and awareness of the situation in the area of operation for interaction with the civilian environment. CIMIC activities are actually at the "intersection" of the military and civilian environment and represent a key border element between military and civilian entities (Guezen 2018, 11). The role of "civil-military cooperation activities is to achieve effective relationships with a variety of civil organizations, but also with key local authorities and population in settlement of conflicts" (Popescu 2019, 56).

The UN Office for the Coordination of Humanitarian Affairs, i.e. UN-OCHA (United Nations Office for the Coordination of Humanitarian Affairs) has defined civil-military coordination (CMCoord). UN-CMCoord "is the essential dialogue and interaction between civilian and military actors in humanitarian emergencies that is necessary to protect and promote humanitarian principles, avoid competition, minimize inconsistency and, when appropriate, pursue common goals. Basic strategies range from cooperation to co-existence. Coordination is a shared responsibility facilitated by liaison and common training" (UN OCHA, 2015). Namely, if UN humanitarian organizations or other UN agencies (from the humanitarian cluster) have appropriate representatives in the area of operation, they can be one of the more important points of contact for CIMIC authorities to address humanitarian issues. Civilmilitary coordination "takes place between the military component and all the civilian components of the UN mission, other members of the UN system and all the other external and internal actors in the mission area" (De Coning 2007, 10). According to De Coning external actors „are all international actors engaged in undertaking humanitarian assistance, conflict prevention, and peacebuilding activities in a given country or conflict system" (De Coning 2007, 10). While internal actors "are all local actors in the country or conflict system where peacebuilding activities take place" (De Coning 2007, 10).

The role of civil-military cooperation in UNIFIL

During the research, a scientific interview was conducted with, Serbian Armed Forces CIMIC officers engaged in the peacekeeping operation UNIFIL in Lebanon. The scientific interview was semi-structured, i.e. the respondents were asked pre-formulated questions. The questions were designed based on long-standing discussions in classes at the University of Defense. Since the questions were open-ended in nature, this allowed for control over the direction and content of the conversation, but also for the scientific interview to yield unexpected data that shed light on the role of CIMIC in peacekeeping operations from a different perspective. This type of scientific interview was chosen because of its flexibility and suitability for the research question. In any case, the interview questions were based on the research question and the framework conceptual model of the phenomenon that underlies the research. Therefore, all this allowed for a more detailed look at CIMIC in peacekeeping operations. Another argument in favor of this research technique is that this type of scientific interview emphasizes the personal experience of the respondents to the greatest extent, which was very important for the research (Ayres 2008).

The scientific interview implied that the respondents were asked three questions:

1. How do CIMIC personnel achieve cooperation with civil environment factors in the area of responsibility of a peacekeeping operation?
2. What are the basic forms of engagement of CIMIC personnel in a peacekeeping operation?
3. Do and to what extent do CIMIC personnel have an impact on the efficiency and success of a peacekeeping operation?

The paper presents only the most important findings obtained during the scientific interview with CIMIC personnel in the peacekeeping operation in Lebanon, which show the very essence of the place and role of CIMIC in peacekeeping operations. Namely, "all CIMIC personnel are obliged to cooperate with civil actors in their areas of responsibility and to report to their functional superiors in the CIMIC chain in order to create a comprehensive system of connections and relationships in the area of operation" (CIMIC COE 2022b). CIMIC personnel in a peacekeeping operation are responsible for "supporting the command in terms of the smooth conduct of the operation, in a way that minimizes the impact of the civil environment on the conduct of the operation" (CIMIC COE 2024). In fact, their activities aim to create a favorable environment for the implementation of the mission mandate.

Based on the assessment of the civilian environment in the area of responsibility of the operation, CIMIC personnel, based on work plans and other planning documents, plan, organize, coordinate, and participate in meetings with representatives of local authorities, religious organizations, representatives of host state authorities, non-governmental organizations, international organizations and other civil environment actors in the area of responsibility of the operation. In this way, possible CIMIC projects and future civil-military cooperation activities are identified. The goal is to assess the state of the civilian environment, identify key civil environment actors, and exchange open information with relevant entities (CIMIC COE 2022b; 2023; 2024).

The civilian component of the UN mission deals with providing assistance to the civilian population through numerous activities. The most important and basic form of engagement of CIMIC personnel in a peacekeeping operation is CIMIC projects, which can achieve the expected effects in a short period of time. CIMIC projects represent one of the basic forms of engagement of military resources through CIMIC activities and are implemented for the purpose of cooperation and the needs of the civilian environment. In addition to projects financed from the UN budget, there are also national projects of the countries participating in the operation that are financed from national budgets. UN projects are implemented in the entire operation zone, while national projects are implemented in the area of deployment of a unit from a particular country. Projects funded by the UN are aligned with the needs of the population and are intended to establish and build trust in the mission, its mandate, and the peace process in general, creating a favorable environment for the implementation of the mandate (DPKO/DFS 2020).

The areas in which projects are implemented are very diverse. Most often, these are projects to build the capacity (development) of local communities and projects to meet the basic needs of the population. They include projects: construction or renovation of health facilities, improvement of health services (various medical equipment for local clinics and hospitals), improvement of the school and education system (equipping schools and community centers in local communities),

development of rescue and firefighting capacities (construction and renovation of fire brigade houses), construction and development of sports capacities (sports fields and sports facilities), environmental protection (waste disposal, afforestation, etc.), development of the local community through projects (purchase of generators and cables for electricity, installation of street lighting, construction of water tanks or water treatment plants, construction of sewage systems with treatment devices, and construction of smaller road sections, etc.) and generally speaking, all other conditions for improving the life and work of the local population (CIMIC COE 2022b; 2023; 2024).

The selection of projects must be aligned with the objectives and mandate of the mission, must be based on the initiative and needs of the local community, and must be accepted by the competent authorities and institutions of the host country. The subject of project implementation: "may also include activities that contribute to the creation of new jobs, training the population for crafts, etc." (CIMIC COE 2022b).

Projects "are identified by CIMIC personnel at the battalion level in the assigned areas of responsibility through regular activities to maintain contact with the civilian environment. They can also be identified and proposed by representatives of local communities or organizations, and must be supported by the heads of local administrative units" (CIMIC COE 2022b). After identifying a possible project, coordination meetings are organized at which the projects are presented, specified, and corrected.
If the project is approved, its implementation is initiated, contracts for the implementation of the project are signed and its implementation is monitored. During implementation, "CIMIC personnel are obliged to carry out controls on the level of implementation, and report on this to the functionally competent elements of the mission" (CIMIC COE 2022b). Good coordination with other CIMIC personnel avoids duplication of projects both in terms of area of operation and in terms of locations where they are implemented.

In addition to projects, CIMIC personnel carry out various activities that represent mutual cooperation between UN forces and representatives of the local community, which does not require the expenditure of funds, which makes them very easy to distinguish from CIMIC projects. Activities most often include: "meetings and contacts with representatives of the local community, medical, dental and veterinary examinations, sports and cultural activities, education of the local population, assistance to the local population, etc." (CIMIC COE 2022b). The implementation of such activities allows the military component to build good relations with certain segments of the local community and thus increase the security of its forces in the area of operation. The CIMIC personnel interviewed point out that medical and veterinary assistance activities are particularly well received by the civilian population, as local governments lack sufficient capacity in this area (CIMIC COE 2024). In carrying out missions and tasks in a peacekeeping operation: "members

of CIMIC personnel at the battalion level are in constant contact with the civilian environment. It often happens that several meetings are held in a short period with representatives of local authorities, organizations, and institutions in order to maintain civil-military relations. Public places and events of the local population are also visited in order to ensure the visibility of the presence of the mission forces" (CIMIC COE 2022b). Furthermore, the interviewed members point out that: "the effects achieved by CIMIC activities have a positive impact on security because their implementation creates direct communication with a larger population in the area of operation" (CIMIC COE 2023).

Some specific activities and projects with specific impact: Activities of the Serbian medical team in southern Lebanon (UNIFIL 2015); Participation of the Serbian Armed Forces in a project aimed to provide support to the local community in Lebanon in "the project, run by the UN mission, aims to promote gender equality and the locals' understanding of the role of women in peacekeeping operations" (Ministry of Defence, Republic of Serbia 2022). In addition, humanitarian efforts during the COVID-19 pandemic were also notable. United Nations Under-Secretary-General for Peace Operations Jean-Pierre Lacroix thanked Serbia for participation in UN peacekeeping operations highlighting that in UNIFIL: "The unit has not only performed its military activities in a highly professional manner, it has also carried out humanitarian efforts to support host communities in their fight against the COVID-19 pandemic" (United Nations Serbia 2021).

The interviewed CIMIC authorities in peacekeeping operations agree that CIMIC has great potential and a great impact on the efficiency and success of contemporary peacekeeping operations because it creates a favorable civilian environment (CIMIC COE 2022b; 2023; 2024).

Conclusions

United Nations peacekeeping has evolved in recent decades. United Nations peacekeeping operations become multidimensional, encompassing military and civilian activities, political affairs, the rule of law, and the protection of human rights. This multidimensionality recognizes the interconnectedness of politics, security, development, and human rights.

In traditional peacekeeping operations, there was a division of responsibilities, with the military responsible for security and civilian organizations for humanitarian and other activities. At that time, their mutual relations were more at the level of coexistence, with occasional coordination of activities or exchange of information on security issues. The evolution of peacekeeping operations and the complexity of the operational environment have led to an increase in the participation of the military component in providing assistance to the actors in the civilian environment.

It is therefore clear that the level of cooperation has also become much higher, as contemporary peacekeeping operations require the active participation of military and civilian capacities. In such an operational environment, CIMIC has gained great importance, and in fact, it can be argued that contemporary peacekeeping operations are unthinkable without adequate CIMIC. During the research, the technique of scientific interview was applied with CIMIC personnel engaged in peacekeeping operations under the auspices of the UN. This methodological technique was chosen due to its particular convenience and the possibility for CIMIC personnel to explain the importance and role of CIMIC in contemporary peacekeeping operations as precisely and scientifically as possible. In the research, the CIMIC officers interviewed in peacekeeping operations were absolutely in agreement that CIMIC has great potential and exerts a significant influence on the efficiency and success of peacekeeping operations, with a particular emphasis on creating a safe environment for the deployed military forces. The research also largely indicated and shed light on the significant potential and opportunities that CIMIC has in the implementation of CIMIC projects in UN peacekeeping operations.

The purpose of CIMIC in a peacekeeping operation is to achieve the objectives of the two parties involved, military and civilian, which also include political, military, civilian, and humanitarian elements. It is cooperation that refers to all measures taken between the military component and the actors of the civilian environment. The most important aspect of civil-military cooperation in peacekeeping operations is the coordination and cooperation between the military and civilian elements in the area of operation. The role of CIMIC is to establish and maintain cooperation with key actors of the civilian environment in the area of operation so as to influence the creation of favorable conditions for the implementation of the mission mandate and the creation of a safe and secure environment. It also aims to create and maintain conditions to support the solutions reached to sustainable peace.

References

Ayres, Lioness. 2008. "Semi-structured interview." In The *SAGE Encyclopedia of Qualitative Research Methods 1*, ed. Lisa M. Given, 810-811, USA: SAGE Publications, Inc.

Civil-Military Cooperation Centre of Excellence [CIMIC COE]. 2022a. *New definitions for CIMIC and for CMI*. Accessed December 2, 2024. https://www.cimic-coe.org/news/definition-CIMIC-CMI/.

__. 2022b. Interview, CIMIC Officer.

__. 2023. Interview, CIMIC Officer.

__. 2024. Interview, CIMIC Officer.

De Araujo Grigoli, Guilherme. 2022. "The Civil-Military Relationship: from Theory to Practice in the United Nations Mission in South Sudan (UNMISS)." *Brazilian Journal of African Studies/Revista Brasileira de Estudos Africanos* 7(13): 105-130.

De Coning, Cedric. 2005. "Civil-military coordination and UN peacebuilding operations." *African Journal on Conflict Resolution* 5(2): 89-118. https://doi.org/10.4314/ajcr.v5i2.39393.

__. 2007. "Civil-military coordination practices and approaches within United Nations peace operations." *Journal of Military and Strategic Studies* 10(1): 1-35. https://jmss.org/article/view/57636/43306.

Eisenhower, Dwight D. 1942. Foreign Relations of The United States: Diplomatic Papers, 1942, Europe, Volume II. 851R.50/29. https://history.state.gov/historicaldocuments/frus1942v02/d501.

Esler, Rory. 2020. "Is the Irish Defence Forces Developing the Necessary Capability to Meet the Operational Requirements of its UN CIMIC Roles? A Case Study of CIMIC Operations in Lebanon." *Journal of Military History and Defence Studies* 1(2): 142-172. http://ojs.maynoothuniversity.ie/ojs/index.php/jmhds.

G**arbino, Henrique, Jonathan Robinson, and João Valdetaro.** 2024. "*Civil-military what*?!." Factsheet repository, Center for Human Rights and Humanitarian Studies, Watson Institute for International and Public Affairs – Brown University and Department of War Studies – Swedish Defence University.

Guezen, Benthe. 2018. "Breaking Down Barriers–Towards Improving Civil-Military Coordination in 'Robust' UN Peacekeeping Operations: A Malian Case Study." Master Thesis. Radboud University Nijmegen: Program in Human Geography, Specialization: Conflicts, Territories, and Identities.

Holshek, Christopher, and Cedric De Coning. 2017. *Civil-Military Coordination in Peace Operations*. Williamsburg: Peace Operation Training Institute.

Langholtz, Harvey J. 2010. *Principles and guidelines for UN peacekeeping operations*. New York: Peace Operations Training Institute.

Lloyd, Gary, and Gielie van Dyk. 2007. "The challenges, roles and functions of civil military coordination officers in peace support operations: a theoretical discussion." *Scientia Militaria: South African Journal of Military Studies* 35(2): 68-94. https://doi.org/10.5787/35-2-38.

Manga, Marius Vasile. 2023. "The security of United Nations personnel in peace missions and operations." *Bulletin of "Carol I" National Defence University* 12(01): 172-180. https://doi.org/ 10.53477/2284-9378-23-15.

Ministry of Defence, Republic of Serbia. 2022. *Participation of Serbian Armed Forces in project aimed to provide support to local community in Lebanon*. Accessed December 2, 2024. https://www.mod.gov.rs/eng/18389/ucesce-vojske-srbije-u-projektu-podrske-lokalnoj-zajednici-u-libanu-18389.

NATO CIMIC & US Civil Affairs Doctrinal Review & Comparative Assessment. 2022. CIMIC Centre of Excellence, Concepts, Interoperability, Capabilities, NATO CIMIC – US CA Synchronisation Project.

Parepa, Laura-Anca. 2013. "Challenges for civil-military cooperation in peace support operations: Examining the framework of comprehensive approaches." *United Nations Peace and Progress* 2(1): 23-48.

Popescu, Eugen. 2019. "Civil-Military Cooperation in nowaday's security environmen." *Bulletin of" Carol I" National Defence University*, no. 01 (March): 52-58.

Radojević, Slobodan, and Srđan Blagojević. 2024. "National interest of the Republic of Serbia for participation of Serbian Armed Forces in peacekeeping operations." *Srpska politička misao – Serbian Political Thought*, 83(1): 141-160. https://doi.org/10.5937/spm83-48311.

UN Peacekeeping. 2024. "Principles of Peacekeeping." https://peacekeeping.un.org/en/principles-of-peacekeeping.

United Nations Interim Force In Lebanon [UNIFIL]. 2015. *Serbian medical team enjoys warm welcome in south Lebanon*. Accessed December 3, 2024. https://unifil.unmissions.org/gallery-1531serbian-medical-team.

United Nations Department of Peacekeeping Operations [UN DPKO]. 2002. Civil-Military Coordination Policy, New York: UN.

__. 2022. Civil–Military Coordination in UN Integrated Peacekeeping Missions. New York: United Nations.

United Nations Department of Peacekeeping Operations / Department of Field Support [UN DPKO/DFS]. 2020. Policy Directive on Quick Impact Projects, New York: UN.

United Nations Office for the Coordination of Humanitarian Affairs [UN OCHA]. Civil-Military Coordination Section [CMCS]. 2015. *UN CMCoord field Handbook*. Geneva: UN.

United Nations Serbia. 2021. *United Nations thanks Serbia for its contribution to peacekeeping*. Accessed December 3, 2024. https://serbia.un.org/en/135770-united-nations-thanks-serbia-its-contribution-peacekeeping.

Wassay, Muhammad Abdul, and Faruzan Anwar Butt. 2022. "CIMIC and Peacekeeping 'Effectiveness': The Role of 'Communication' as a Critical Interface in Evolving UNPKO Dynamics." *NUST Journal of International Peace & Stability*, 1-14. https://doi.org/10.37540/njips.v5i1.113.

ACKNOWLEDGEMENTS

This paper was written as a part of the pre-research in scientific project funded by the Ministry of Defence, Republic of Serbia, number: VA-DH/1/24-26 "Value orientations and attitude towards the tradition of the cadets of the Military Academy".

CONFLICT OF INTEREST STATEMENT

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

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Impact of new fire support capabilities from a joint functions perspective

LTC Adrian MIREA, Ph.D. Candidate*
*"Carol I" National Defence University, Bucharest, Romania
e-mail: mirea.adrian82@gmail.com

Abstract

The article highlights the usefulness of the operational framework described by the joint functions to understand the impact that an available capability has on the operation from an actional point of view. At the same time, this framework can also be exploited for the purpose of identifying a need for capabilities at the level of the current joint force in order to be able to accomplish the assigned missions. In order to argue the above, I have focused on a fire support capability that has recently become part of the national armed forces structures - the M142 HIMARS (High Mobility Artillery Rocket System). If in the first part of the article I briefly detailed aspects of the operational framework described by the joint functions, in the second part I presented a reasoned perspective on the impact that the capabilities of HIMARS systems have on the way of conceptualizing operations. The article aims to argue, through a concrete example, the possibility of using the operational framework described by the joint functions to understand the full potential of an existing or prospective capability for national armed forces structures.

Keywords:
joint functions; HIMARS systems; fire support; operational framework; capability.

Article info
Received: 25 October 2024; Revised: 18 November 2024; Accepted: 29 November 2024; Available online: 17 January 2025

Citation: Mirea, A. 2024. "Impact of new fire support capabilities from a joint functions perspective." *Bulletin of "Carol I" National Defence University*, 13(4): 126-137. https://doi.org/10.53477/2284-9378-24-53

The integration of new fire support capabilities under current or forward-looking equipping programs also requires, in my view, an understanding of how the military commander can exploit their full potential in operations. Warfighting functions provide a useful context for conceptualizing the way new capabilities can be exploited in a timely manner, according to the operational needs of the force structures that possess or will possess them at a given point in time. Through this article, I have aimed to highlight a useful way to understand the impact of new fire support capabilities of national armed force structures and how the commander and his staff can conceptualize the exploitation of the new capabilities they offer in planning and conducting the operations of their force structures.

For the completion of this paper, I considered the method of documentary analysis in order to systematically select, review and evaluate public (unclassified) sources of information. In this manner, I aimed to illustrate in a synthesized way a perspective on the potential implications of the integration of new military capabilities at the national level. I considered it sufficiently relevant to address the influence of a limited number of new or prospective military equipment capabilities using the framework in which combat functions manifest since, in my view, the way of constructing the perspective can be extrapolated to other types of equipment, capabilities or services available to national armed forces structures.

Joint functions are a tool, at the disposal of the commander and his staff, used in particular to ensure a holistic approach to all aspects of an operation and to visualize the specific activities of the force structures available in the operational framework created. Joint functions are basically a description of the capabilities available to the force structures. The concrete requirements of the joint force for the conduct of an operation are determined by the commander through the joint functions (NATO 2022a, 105). From this point of view, the joint functions come to argue the current requirements of a joint force but also the need for armed force structures to have modern capabilities, adapted to the current confrontation environment.

The operational framework described by the joint functions

Within both NATO (NATO 2022a, 105) and national perspective (SMG 2011, 70) (SMG 2014, 26) the joint functions are:

- fires and maneuver;
- command and control (C2);
- intelligence;
- force protection;
- information operations (INFO OPS);
- sustainment;
- civil-military cooperation (CIMIC).

It should be noted that, differently from NATO regulations, at the national level there are seven joint functions since manoeuvre is associated with fires in a single function. In the following lines, I will briefly present the main ideas of each of the joined functions in order to address them in the second part of this paper in interpreting the potential impact of new capabilities.

Fires and manoeuvre (*manoeuvre and the application of firepower* according to Romanian Army doctrine) integrate, from a national perspective as mentioned, two joint functions according to NATO doctrines. The main purpose of *manoeuvre* is to obtain an advantageous position in relation to the enemy that would allow the threat or application of force against him. At the operational level, manoeuvre is the process by which combat power is concentrated where it would have a decisive effect in preventing, disrupting or neutralizing enemy operations (NATO 2019, 1-21). Although usually manifested physically, the manoeuvre can affect the morale of enemy forces by creating uncertainty, confusion and paralysis. Fire, applied by structures of two or more categories of armed forces, has as its main purpose to influence the enemy's combat capability. The effects of fires are mainly physical, but they can also affect the psychological and morale components of combat power, thus having an impact on the enemy's will to fight.

Command and control (C2) as a joint function is the exercise of authority by the commander over available forces to accomplish the mission. Operations are characterized by centralized planning and direction to ensure unity of effort, and decentralized executive authority down to the lowest echelon capable of effectively employing force structures. A representative element is the command-and-control architecture which, in today's operating environment, is dependent on capabilities exploiting the increasingly congested and contested electromagnetic spectrum (NATO 2022b, 49).

The role of *intelligence* is to ensure a continuous and coordinated understanding of the confrontation environment, supporting the commander by identifying the conditions necessary to accomplish objectives, avoiding undesirable effects and assessing the impact of enemy action, own forces or other actors on the concept of operation. The *intelligence* joint function is an essential tool for the conduct of the decision-making process as it integrates the activities of the commander, staff and collection elements to generate the required intelligence products resulting from the information cycle (direction-collection-processing-dissemination).

Force protection is a function focused on eliminating or minimizing the vulnerability of personnel, equipment, facilities, operations and activities to potential threats or hazards, to ensure freedom of action and operational effectiveness in accomplishing the mission. Force protection is a responsibility of commanders at all hierarchical levels but also a fundamental ongoing responsibility of all personnel. Representative aspects of this function include air defence, CBRN

(Chemical, Biological, Radiological and Nuclear) defence, military engineering and operational security.

Information Operations (INFO OPS) as a joint function integrates those actions and activities that produce effects on the understanding and perception, the will to fight and the capabilities of target entities in order to assist in the accomplishment of the set objectives. Key enablers of this function include psychological operations, deception, electronic warfare and physical destruction (SMG 2014, 33).

Sustainment refers to the coherent provision of the necessary support for the conduct of the operation until mission accomplishment. This support mainly concerns the provision of resources (human and material), medical support and military engineering. Rehabilitation, resupply and regeneration of force elements are outcomes of sustainment and play an important role in maintaining the required level of combat capability. The degree of sustainment has an impact on the tempo, duration and intensity of all types of operations.

Civil-military cooperation (CIMIC) is the coordination and cooperation of military commanders with civilian actors in the area of operations to accomplish the force's objectives. Through this function, the commander can create and maintain conditions favourable to the accomplishment of his mission by exploiting moral, material or tactical advantages to the detriment of the enemy. Civil-military interactions are an important tool in achieving strategic and operational level objectives as civilian actors in the area of operations can have an impact on the outcome of the conflict situation or crisis.

Through the operational framework described by the joint functions, the commander combines the actions and activities of the force structures to generate effects aimed at influencing the enemy's ability to understand, the level of capabilities available to him and his will to fight. Similarly, the activities and actions of the available force structures produce effects with the potential to influence the enemy's ability to understand, the level of capabilities and the will to fight from the perspective of friendly forces or other actors in the area of responsibility.

The capabilities available at force structure level define each of the joint functions but, taken in isolation, these capabilities can be leveraged across multiple functions. The commander, in order to accomplish his mission, may choose from a multitude of available capabilities and combine or integrate them in a number of ways to accomplish the combined functions listed above. He will detail in the operation order the concrete way in which the available forces and assets are to be employed, but they are not exclusively associated with a single function. An action of an available force or capability can and will be exploited within more than one joint function.

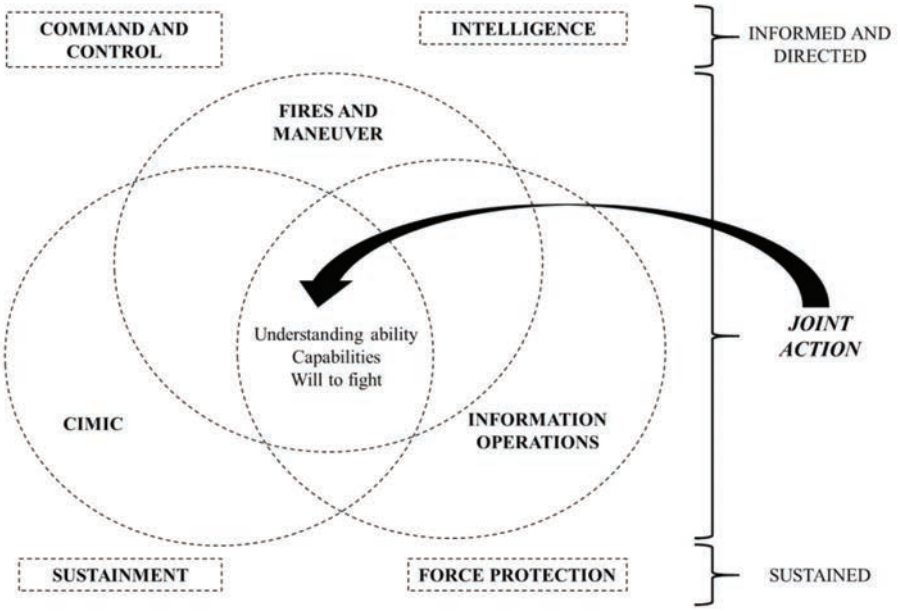


Figure 1 Actional framework described by the joint functions
Source: Adaptation from AJP-01 Allied Joint Publication, 2022, p. 106.

The impact of new fire support systems on performing joint functions

The practical conditions under which the combat power of a force can be effectively applied are related to an understanding of the conflict nature and the context in which it is manifested, the specific operating environment, the target entities with existing threats, and the capabilities available for friendly structures, the enemy or other actors present in the area of responsibility.

More often than not, the increased capabilities of modern fire support systems are visualized to have implications in a geographic framework of the action, through the increased maximum range at which they can strike targets - in the deep, close and rear area of operations. An example of this is the equipping of the Romanian Army's land force structures with M142 HIMARS (High Mobility Artillery Rocket System), which, at first sight, brings to mind the maximum range at which they can engage targets - 70 km (for GMLRS – Guided Multiple Launch Rocket System) and 300 km (for ATACMS – Army Tactical Missile System). An illustrative representation of the impact that the maximum range of fire support systems can have on the operational environment can be found in *Field Manual FM 3-0 Operations* from 2022.

This representation shows the influence of the maximum range of fire support systems (available to both sides) on an area of operations perspective at the operational and tactical level.
Given the full range of possibilities offered by HIMARS (increased range compared to the artillery systems they have replaced, improved accuracy, a greater variety of potential munitions, the advantage of minimizing possible collateral effects, etc.) we

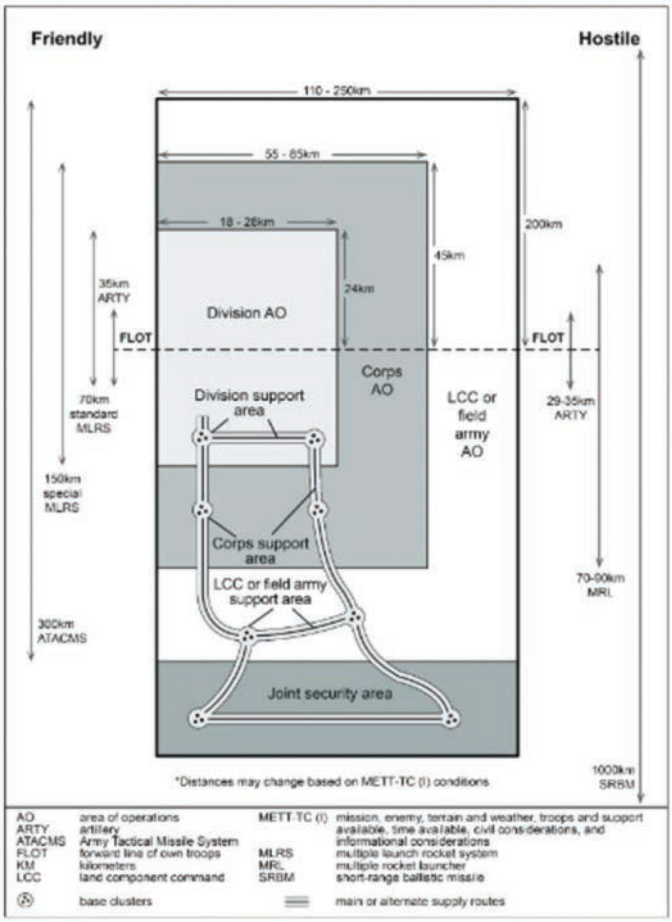


Figure 2 Doctrinal model of representing front and depth dimensions
Source: Field Manual FM 3-0 Operations, 2022, p. 6-8.

can consider multiple ways of exploiting these systems in the operational framework described by the joint functions.

I have presented below a personal perspective on equipping national land forces with HIMARS systems where I have integrated the main aspects in the form of a SWOT analysis.

Although only certain types of ammunition have been procured nationally (Defence DataBase 2024), this paper has considered HIMARS systems as platforms with the potential to utilize the full range of ammunition available to such systems. Another aspect worth mentioning is that in detailing the perspective of the contribution and integration of HIMARS systems into friendly forces' joint functions, I have also addressed some aspects regarding the potential for disrupting enemy joint functions.

Fires and manoeuvre

The main contribution of HIMARS systems in the joint function *fires and manoeuvre* is the potential to diminish the combat capability of enemy force structures, either directly by destroying various military equipment or indirectly by influencing the psychological and morale status of enemy troops. The accuracy of the munitions fired

TABLE NO. 1

SWOT analysis regarding equipping national land force structures with HIMARS

STRENGTHS	WEAKNESSES
- HIMARS are validated systems as effective in recent conflicts (Iraq, Afghanistan, Ukraine) - Equipping with such systems helps deter armed aggression against Romania - They can provide fire support in both joint and multi-domain operations - They have a high degree of mobility, also being air mobile, offering increased flexibility - They ensure a high degree of technical interoperability with allies in terms of command-and-control systems - Capable of *shoot and scoot* fire missions, ensuring a high degree of survivability in today's confrontation environment - Can accurately engage targets at considerably longer ranges than existent conventional artillery systems - They use the advanced fire support command and control system - IFATDS (International Field Artillery Tactical Data System) which allows automated fire planning, coordination and execution - They have an integrated logistics system with containerized ammunition and the possibility of mechanized loading (Forțele Terestre Române 2024) - They can use a wide variety of ammunition with different payload types - Munitions are designed to minimize the risk of casualties or collateral damage - Launched munitions have high velocity and a low radar signature, which renders them difficult to detect and intercept as they are hard to distinguish from other conventional munitions	- The need for dedicated resources in order to ensure physical protection as well as anti-aircraft/anti-rocket protection of HIMARS systems, as they are high pay-off targets for a potential enemy in all types of operations - The need to associate electronic warfare platforms and high-performance radars with HIMARS systems in order to detect and combat drones, in particular reconnaissance drones, providing them with multispectral protection adapted to a modern conflict - In my view, multispectral protection also involves the implementation of effective modern measures suitable for protecting these systems, such as multispectral camouflage or the use of 'convincing' models or replicas of HIMARS platforms - Enemy jamming along the trajectory or in the target area can have effects on the accuracy of munitions (Marquardt, Bertrand and Cohen 2023) - The operation of HIMARS systems is dependent on the provision of foreign-sourced contingency materiel, in particular munitions. This can be problematic in crisis/conflict situations when demand may be high and resource allocation will be prioritized.
OPPORTUNITIES	**THREATS**
- The potential of locally supporting HIMARS systems operability through Aerostar S.A. Bacău (Lockheed Martin 2024) - Participation in multinational exercises exploiting Romania's membership in the ASCA community (Artillery System Cooperation Activities) (Orjanu 2023) - Enables access to emerging munitions for such systems (e.g.: Extended Range GMLRS with a maximum range of 150 km and Precision Strike Missiles with a maximum range of 499 km) including munitions with trajectory-correction systems, active immediately after launch, to make them harder to identify with counter-battery radars	- The risk of partially harnessing the potential of HIMARS systems due to the limitations of current national ISR (Intelligence, Surveillance and Reconnaissance) capabilities - Reduced operational effectiveness of HIMARS systems over time as a result of lessons identified in the Russian-Ukrainian conflict - The development of new capabilities or implementation of new tactics to counter the effects of HIMARS as a result of lessons identified (Newsweek 2024; Goldstein and Waechter 2023) - Reliance on satellite information for target acquisition but also for GPS guidance of munitions, while anti-satellite warfare capabilities exist worldwide (VPK News 2023)

by HIMARS systems can be utilized primarily on fixed targets, such as infrastructure elements used by the enemy or concentrations of forces - in certain directions of effort, at objectives or located in various areas. Considering the variety of munitions (including submunitions) (Defence DataBase 2024) that can be launched by HIMARS systems, we can consider a wide range of effects on the enemy in direct support of friendly manoeuvre structures.

From the enemy's perspective, the manoeuvre and joint fire function are disrupted by the ability of HIMARS systems to rapidly execute accurate fire on high-value targets. Thus, by employing submunition strikes (including anti-armour mines) in certain areas or at certain times of the operation, various effects on the enemy's manoeuvre forces can be achieved such as disrupting offensive actions, and blocking or delaying the introduction of reserves into the battle. I mention here the direct contribution of HIMARS systems in Donbas to blocking the offensive of Russian forces in the

Bakhmut-Kramatorsk direction in July 2022 (Nistorescu 2024, 79). Another aspect of the deployment of HIMARS systems that may disrupt this joint enemy function is also, in my view, the polarizing effect of enemy fire support assets specifically intended for HIMARS detection and counteraction throughout the operation.

Another important contribution of HIMARS systems to the disruption of the enemy's joint function *fires and manoeuvre* is their high proficiency in executing counterbattery fires (Global Defense News 2023). The effectiveness of HIMARS systems in such situations is based on their high mobility, the availability of an automated fire control system, and the ability to execute *shoot-and-scoot* fire missions, all in conjunction with high accuracy and lethality on target. Another advantage in this area may also be the development and use of munitions with trajectory correction systems immediately after launch, to make it impossible to accurately detect firing positions with counter-battery radars (Kadam 2022).

Command and control

The joint function *command and control* is enhanced by equipping force structures with HIMARS systems in several ways. One of these is the prospect of effective command and control of fire support through the exploitation of IFATDS. The speed with which the automated planning and execution of fire missions is carried out has implications on the ability to react, in the form of counter-battery fire, against enemy fire support systems aimed at disrupting the exercise of command and control at the joint force level. The reaction capability can also be exploited against targets of opportunity arising in the dynamics of action, especially those classified as TST (Time Sensitive Target), where HIMARS may be the only effective capability available to the commander.

Given the *command-and-control* function from the enemy's perspective, HIMARS systems have proven to be particularly effective in hitting command post targets (BBC 2022), thereby disrupting the functionality of enemy command and control systems at different tactical echelons.

Intelligence

The capabilities of HIMARS systems are integrated and assist the joint function *intelligence* by contributing to the operational picture, capitalizing on the characteristics of the modern IFATDS fire command and control system and exploiting target acquisition data and information.

Disrupting the enemy's *intelligence* function with HIMARS systems can be achieved by physically destroying equipment intended for data transmission or data collection such as, for example, communications centres (Kadam 2022) or counter-battery radars (New Voice of Ukraine 2023). The exploitation of HIMARS systems as part of deception plans can contribute to degrading the enemy's ability to understand the real operational situation by stimulating sensors and deliberately providing certain information such as, for example, shifting the main effort of the force in a certain

direction by deploying and employing launch positions for this purpose. As an example, I would like to highlight the role of HIMARS systems from 2022 in the Russo-Ukrainian conflict, as they contributed to misleading the enemy and drawing attention to the province of Kherson, an action followed by the counter-offensive in Kharkov (Toroi 2024, 34).

Force protection

The impact of equipping with HIMARS systems on the joint function *force protection* can be understood, in my view, in two aspects, one positive and one negative. The positive aspect is primarily the high capability of HIMARS systems to effectively combat enemy strike systems from a distance, particularly those that pose a high risk to friendly force structures - such as tactical assets with WMD capabilities.

The negative aspect would be, in my view, the need to allocate additional or dedicated resources for direct protection and close defence of HIMARS systems, as well as for their air and missile defence throughout the entire operation. This is also a consequence of the fact that, as stated earlier, the HIMARS systems available to a force are high pay-off targets for any potential enemy.

From the enemy's perspective, the *force protection* function is disrupted primarily by the constant need to mitigate the effects of a potential HIMARS attack, which may occur at considerable distances from the front line. Thus, in order to protect important enemy infrastructure elements, concentrations of forces or resources of any type, or to protect other various objectives in rear areas of operations, the enemy will have to take some specific measures and allocate additional resources (electronic warfare or air and missile defence) to mitigate the effects of HIMARS engagement.

Information Operations (INFO OPS)

The availability of HIMARS systems at the joint force level and their successful employment during operations can be exploited in information operations to boost the will to fight and the morale of friendly troops. An elementary example in this area can be the promotion of successful HIMARS actions among friendly forces. At the same time, equipping forces with HIMARS and the direct implications of this, such as pushing concentrations of enemy assets further away from the front line, can have demoralizing effects on enemy force structures in the close area of operations (Kosoy 2024).

Another aspect, also mentioned in the joint function *intelligence*, is to capitalize on the status of HIMARS systems as a high pay-off target for the enemy in plans to mislead them. The contribution of HIMARS to degrading the enemy's ability to understand the operational situation can be significant.

As a characteristic element of the joint function *information operations* from the enemy's perspective, I mention the enemy's focus on propaganda aspects, promoting the destruction of HIMARS systems (Tass 2024) or the unconventional manner of their use - against civilian population or objectives (Avia.Pro 2022). The disruption

of this joint function can be achieved, first of all, by becoming aware of these aspects and then implementing countermeasures or exploiting them in the framework of friendly information operations.

Sustainment

From a *sustainment* point of view, equipping forces with HIMARS systems have a major impact on the geometry of the operating environment. While from a friendly operations perspective, the main contribution to sustainability is, in my view, countering fire support systems that could disrupt the flow of resources. Regarding enemy operations, HIMARS systems have demonstrated a high potential to affect their sustainability. The maximum range at which HIMARS systems can accurately and effectively engage targets has been intensively leveraged (and publicized) in the Russo-Ukrainian conflict as they were used to strike infrastructure elements, force concentration areas, ammunition depots, or Russian soldier training bases (Kosoy 2024). Thus, we could observe that equipping friendly force structures with HIMARS systems may lead to a revision of the enemy's way of deploying resources at considerable distances from the front line in order to remove them from the HIMARS engagement range.

Civil-military cooperation (CIMIC)

The advantage of using munitions that are constructively aimed at reducing the risk of casualties or collateral damage can be exploited in this joint function to strengthen support for the cause from the civilian population existing in the area of operations. Moreover, the population in the territory occupied by the enemy can be an important source of information regarding his use of military equipment or the conduct of activities by his forces, information which can also be exploited in the planning and execution of fire missions with HIMARS systems.

Concerning the disruption of the enemy's *civil-military cooperation* joint function, special attention needs to be paid to the relationship of proportionality between these functions of the conflicting parties. Thus, the progress achieved by the actions of friendly forces in the functional area of civil-military cooperation strengthens this joint function while, obviously, securing enemy disadvantage.

Conclusions

Exploiting the operational framework described by the joint functions can be done beyond their basic role - the tool of the military commander and his staff to ensure a comprehensive approach to the aspects of an operation. Considering that the way joint functions are accomplished in an operation is also a description of the capabilities available to the force, it is possible to argue on their basis some new needs, by solving which mission fulfilment is facilitated in the current confrontation environment.

Joint functions can provide a framework for understanding and realizing the potential of available capabilities to the military commander, but at the same time,

these functions can also provide the requirements of national force structures given the missions they have or may have in a given context. Moreover, by conceptualizing the performance of these functions at the level of a potential adversary or other actor present in the area of operations, we can have a thorough understanding of the potential of the capabilities available to them, which can be exploited both in understanding the confrontation environment as a whole and in determining the centres of gravity for targeted entities.

Through the example used in this paper - the equipping of national land forces structures with HIMARS systems - I have argued a useful way, in my view, to substantiate how to capitalize on existing or prospective capabilities. At the same time, in writing this paper, I have presented and argued a perspective on the impact of equipping national armed forces structures with HIMARS systems by addressing their contribution or influence on the fulfilment of each joint function in particular with examples from the ongoing Russo-Ukrainian conflict.

References

Avia.Pro. 2022. "ВСУ показали особенность применения РСЗО Himars в условиях контрбатарейной борьбы" *(The AFU showed the peculiarity of using Himars MLRS in the conditions of counter-battery combat).* https://avia.pro/news/vsu-pokazali-osobennost-primeneniya-rszo-himars-v-usloviyah-kontrbatareynoy-borby.

BBC. 2022. "Ukraine: What are Himars missiles and are they changing the war?" https://www.bbc.com/news/world-62512681.

Defence DataBase. 2024. "M142 HIMARS multiple rocket launcher". https://defencedb.com/profile_page.php?item_id=16.

Forțele Terestre Române. 2024. "Sistemul de rachete cu lansare multiplă M-142 HIMARS". https://forter.ro/inzestrare/sistemul-de-rachete-cu-lansare-multipl%C4%83-m-142-himars.

Global Defense News. 2023. "Using HIMARS Ukrainian forces destroy five Russian MSTA-S howitzers in key counter-offensive". https://armyrecognition.com/focus-analysis-conflicts/army/conflicts-in-the-world/russia-ukraine-war-2022/using-himars-ukrainian-forces-destroy-five-russian-msta-s-howitzers-in-key-counter-offensive.

Goldstein, Lyle, and Nathan Waechter. 2023. *The Diplomat.* Iunie 22. Accessed August 11, 2024. https://thediplomat.com/2023/06/china-considers-countermeasures-to-us-himars-missile-system/.

Kadam, Tanmay. 2022. *Kudos HIMARS! Russian Military Experts Say US Systems Are Confusing Counter-Battery Ops By Changing Trajectory.* https://www.eurasiantimes.com/kudos-himars-russian-military-experts-say-us-systems-are-confusing-counter-battery-ops-by-changing-trajectory/.

Kosoy, Daniel. 2024. "HIMARS, Ukraine's Original Game Changer." *United24 Media*. https://united24media.com/war-in-ukraine/himars-ukraines-original-game-changer-1613.

Lockheed Martin. 2024. *Aerostar and Lockheed Martin open the first European HIMARS Sustainment Centre in Romania.* https://news.lockheedmartin.com/2024-05-30-aerostar-and-lockheed-martin-open-the-first-european-himars-sustainment-centre-in-romania?_gl=1*1scrj9n*_gcl_au*NDM3NzExMjQwLjE3MzEwMDcxNzc.

Marquardt, Alex, Natasha Bertrand and Zachary Cohen. 2023. "Russia's jamming of US-provided rocket systems complicates Ukraine's war effort." *CNN.* https://edition.cnn.com/2023/05/05/politics/russia-jamming-himars-rockets-ukraine/index.html.

NATO. 2022a. *Allied Joint Doctrine AJP-01.* NATO Standardization Office.

—. 2022b. *Allied Joint Doctrine for Land Operations AJP-3.2.* NATO Standardization Office.

—. 2019. *Allied Joint Doctrine for the Conduct of Operations AJP-3.* NATO Standardization Office.

New Voice of Ukraine. 2023. *HIMARS strike destroys rare Yastreb-A counter-battery radar in Russian Rear – video.* https://english.nv.ua/nation/video-of-himars-destroying-russian-yastreb-a-counter-battery-radar-in-donetsk-oblast-50436872.html.

Newsweek. 2024. *Strikes on Ukraine's Most Prized Assets Raise Alarm.* https://www.newsweek.com/ukraine-russia-strikes-helicopters-abrams-bradleys-1879148.

Nistorescu, Claudiu-Valer. 2024. "Asimetrii generate de noile sisteme de armament și rolul lor în obținerea succesului pe câmpul de luptă. Efectele generate de sistemul HIMARS în conflictul din Ucraina." *Buletinul Universității Naționale de Apărare „Carol I"* 13 (3): 72-83.

Orjanu, Gheorghiță. 2023. „HIMARS deschide uși. Artileria Armatei României a intrat în «clubul select» ASCA. SUA – rol cheie în primirea României în ASCA." *Defense Romania.* https://www.defenseromania.ro/himars-deschide-usi-artileria-armatei-romaniei-a-intrat-in-clubul-select-asca-sua-rol-cheie-in-primirea-romaniei-in-asca_622036.html.

SMG. 2011. *Doctrina Armatei României SMG-103.* București: MApN.

—. 2014. *Doctrina pentru operații întrunite a Armatei României SMG/ PF-3.* București: MApN.

Tass. 2024. *Russia's strike destroys four HIMARS launchers, 35 foreign personnel in Ukraine ooperation.* https://tass.com/politics/1814677.

Toroi, George-Ion. 2024. "A theoretical analysis of the art of deception." *Strategic Impact* (No. 2): 25-47.

VPK News. 2023. *The Russian Armed Forces revealed the weak points of HIMARS.* https://vpk.name/en/714706_the-russian-armed-forces-revealed-the-weak-points-of-himars.html.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Measures against the financing of "lone wolves" and small terrorist cells in Europe

Svetoslav YORDANOV, Ph.D. Candidate*

*Rakovski National Defence College, Sofia, Bulgaria
e-mail: yordanov_sv@yahoo.com

Abstract

This article examines the modern trends of radicalization and terrorism and researches the contemporary sources and methods of terrorist financing. The paper focuses on the emergence of new risks and threats to the European security system, such as the activity of "lone wolves" and small terrorist cells. The purpose of the publication is to study the financing mechanisms of small independent terrorist organizational units and to propose measures against them.

Keywords:

counterterrorism; "lone wolves"; small terrorist cells; radicalization; terrorist financing; European jihadists; far-right extremism.

Article info

Received: 12 November 2024; Revised: 28 November 2024; Accepted: 6 December 2024; Available online: 17 January 2025

Citation: Yordanov, S. 2024. "Measures against the financing of «lone wolves» and small terrorist cells in Europe." *Bulletin of "Carol I" National Defence University*, 13(4): 138-151. https://doi.org/10.53477/2284-9378-24-54

The development of contemporary terrorism depends directly on the dynamics of geopolitical processes, the struggle for natural resources, the strengthening of social inequality, the migration of large groups of people, the speed of the adoption of high technologies, as well as the activation of frozen armed conflicts and the emergence of new ones.

Three events of the last five years can be rightly argued to shape the future trends of radicalization and terrorism, both globally and in Europe in particular. *The first* is the final defeat of DAESH (the Arabic name for the terrorist organization "Islamic State") in the territories of Syria and Iraq as a quasi-state terrorist structure in 2019 by the Global Coalition. *The second* is the return of the Taliban to power in Afghanistan in August 2021 after the withdrawal of NATO and US forces and the subsequent proclamation of the Islamic Emirate of Afghanistan. *The third* is the multi-pronged terrorist attack carried out by Hamas forces and other Palestinian militias on Israel on October 7, 2023, in which over 1,100 people died and 250 were taken hostage. The consequences are increased confrontations between different ethnic and religious communities, an increase in the flow of returning foreign fighters to Europe (CTED 2024), and an overload of the socio-economic systems of the countries of the Old Continent.

In Europe, cases of extremist and terrorist acts committed by self-radicalized individuals acting independently or in small groups, without having a direct connection with an established terrorist organization and without being under its operational leadership, are becoming increasingly common. Information about the sources and methods of their financing is often lacking, which makes it difficult to study their typology and build an appropriate system of measures to counter them. In turn, this also necessitates the need to study the discussed problem.

The massive street fight between two warring factions of Eritrean immigrants in The Hague (Netherlands) in February 2024 (Amalaraj 2024), the acts of violence between Turkish citizens and Kurdish supporters of the PKK (Kurdish Workers' Party) in eastern Belgium in March 2024 (Anadolu Agency 2024), as well as the clashes between Israeli football fans and Palestinian protesters in early November 2024 in Amsterdam (Netherlands) (Al Jazeera 2024), are just some of the manifestations of extremism resulting from the growing ethnonational confrontation in Europe.

The purpose of this publication is to analyse the nature of small independent terrorist organizational units and to formulate solutions to improve the countering of their financing. Three *main research tasks* are identified to achieve the goal: to study the mechanisms of functioning of "lone wolves" and small terrorist cells; to examine the sources and methods of their financing; and to propose measures to counter the financing of "lone wolves" and small terrorist cells.

The object of the study is the terrorists known as "lone wolves", as well as small terrorist cells (composed of two to three people) in Europe, and *the subject* of the

study is represented by the ways to counter the financing of small independent terrorist organizational units.

The research is disciplined by limiting itself to examining cases of financing of "lone wolves" and small terrorist cells professing far-right or Islamist ideology.
The main scientific methods used are systematic analysis, document study (reports from institutions such as Europol, Financial Action Task Force and the U.S. Department of State) and exploratory "case study".

General characteristics of "lone wolves" and small terrorist cells

The analysis of terrorist activity on European territory for the last five years according to reports by Europol (EUROPOL 2019, 2020, 2021, 2022, 2023) and the U.S Department of States (U.S. Department of State 2019, 2020, 2021, 2022) shows that the majority of attacks are carried out by self-radicalized actors who carry out acts of violence that are not planned, prepared and organized by "operational officers" of a specific terrorist organization. This phenomenon is observed in terrorism of different ideological and political bases, but mostly *far-right* and *Islamist* ones.

According to the periodic information and analytical bulletins of the Research Centre for Extremism and Terrorism of the Rakovski National Defence College (Research Centre for Extremism and Terrorism 2023, 2024) over the last two years, at least ten of the terrorist attacks carried out on the territory of Europe were perpetrated by "lone wolves" or members of small terrorist cells, and the cases of prevented terrorist acts planned by such actors are over twenty.

According to researchers from the International Centre for Counter-Terrorism – The Hague, the term "lone wolf" became known in the late 1990s, when it began to be used for individuals who carry out terrorist activities without being hierarchically affiliated with a specific terrorist organization (Bakker and Graaf 2010), and according to a report by the U.S. Department of Justice, the tactics and methods of "lone wolves" are independently selected without external guidance (Hamm and Spaaij 2015).

Based on research conducted by the Royal United Services Institute for Defence and Security Studies (Keatinge and Keen 2017), the following characteristics can be deduced, relevant to both terrorist organizational units ("lone wolves" and small terrorist cells) under consideration:

- Terrorists self-radicalize without the direct influence of recruiters.
- Terrorists have not participated in combat operations in conflict zones.
- Terrorists do not maintain contact with members of a specific terrorist organization.

- Terrorists independently plan and prepare their attacks, as well as select their targets.
- Terrorists do not use external sources of funding relevant to specific terrorist groups.
- The motivation for carrying out the terrorist attack is the support of a specific ideological and political cause.

When analysing the nature of "lone wolves" and small terrorist cells, the issue of radicalization is essential. The phases of this process do not differ in any way from the standard stages of radicalization that every rank-and-file member of a terrorist organization goes through. Based on Malcolm Nance's (Nance 2016) classification, seven main stages of radicalization can be specified: interest; praise; solidarity; isolation; identification; pledge of allegiance; and conscious readiness to commit a violent act. These phases can be attributed to the levels of psychosocial changes that occur in the radicalizing individual, as described by Petar Marinov (Marinov 2022).

The self-radicalized individuals' interest in a specific terrorist ideology is generated by a sense of social injustice, which grows into a firm determination to do justice and accumulates suppressed anger.
This is followed by admiration for the deeds of famous terrorists, who begin to define themselves with various euphemisms such as "rebel", "hero", "defender", and "warrior of God", as a result of which the future terrorist reaches extremes in his assessments and perceptions of reality.
A desire for solidarity with the activities of the terrorist organization arises, rejection of any alternatives and forms of discussion, with the professed ideology being declared the only possible one.

The next stage is associated with self-isolation, since the generally accepted boundaries of morality and laws of society already contrast with the attitudes of the radicalizing individual, and alienation is associated with an unwillingness to communicate with people who express different opinions.
The moment comes when the person begins to identify with the fighters of the terrorist organization he sympathizes with. In order to demonstrate his closeness, he undertakes changes in his appearance (clothing, hairstyle, tattoos) and his manner of communication (way of expression), as well as trying to apply in his daily life the norms of the ideology of the terrorist group he follows, trying to impose them on others by means of verbal aggression.
Pledge of allegiance to a particular terrorist organization is a turning point since the person has already made a final decision to dedicate himself to the terrorist cause, to set a personal example and to make a contribution.

The final phase is expressed in the conscious choice to participate in an act of violence and accept the position of power as the only option for achieving the goals of the terrorist ideology.

The environment in which the described process of radicalization takes place in "lone wolves" and small terrorist cells is concentrated primarily in the online space. The characteristics of this environment include:

- Easy accessibility
- Audio-visual impact of perceptions
- Relative anonymity
- Diversity of content
- Opportunity to find like-minded people
- Rapid sharing of information in real-time
- Globalization of communication

In recent years, there has been a worrying trend of self-radicalization of minors in online space through participation in video game platforms, which are usually associated with virtual violence and the use of virtual firearms. The most dangerous in terms of radicalization are those "action games" in which the application of violence is from the first person, i.e. the computer game interface allows the player's point of view to coincide with the video projection of the virtual character. In this way, human behavioural patterns are subconsciously affected, and the boundary between the virtual and the real becomes thinner. Once rejected in the virtual space, moral inhibitions can more easily be overcome in real life, and violence can be transferred there. It should be noted that there are also video games created by some terrorist organizations that purposefully incorporate extremist content and symbols developed by specialists in the field of psychological operations into their audio-visual presentations.

A "lone wolf" is understood to be an autonomously acting terrorist who independently carries out all activities related to setting goals, planning, preparing and organizing a terrorist attack.
A small terrorist cell is characterized by a similar pattern. In terms of its size, it consists of two or three individuals who reach a mutual agreement to carry out a terrorist act, and for this purpose, they get organized. There may be various hierarchical, functional and communication links between these individuals.
The agreement can be established both between complete strangers and between relatives or friends. In all cases, they share a common ideology and have collectively agreed to use the means of deliberate violence to enforce it.

Three main types of self-radicalized *small terrorist cells* can be proposed based on the number of their members and their interconnectedness (Figure no. 1).

Dyad. This is the smallest terrorist cell, consisting of two members (terrorist 1/ T1 and terrorist 2/ T2). Most often they have friendly or family relationships (husband-wife). These terrorists may share common interests and have a stable emotional connection with each other, which guarantees trust, loyalty and dedication to the cause. The Dyad is the most difficult small terrorist cell to detect by law enforcement agencies.

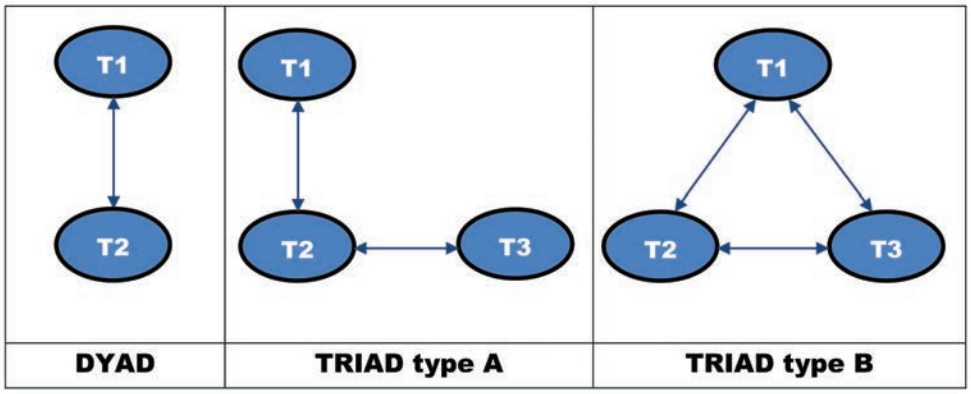


Figure 1 Architecture of small terrorist cells
Source: by the author

Triad type A. This terrorist cell consists of three members, not all of whom maintain direct communication links with each other. For example, *terrorist 1 (T1)* is known to *terrorist 2 (T2)* and the two are in direct communication, while *terrorist 3 (T3)*, who is *T2's* wife, does not know *T1*. However, the three members operate within a common organizational structure, share a common cause and together plan and prepare to commit a terrorist act. In *Triad type A*, the probability of distributing functional responsibilities is highest.

Triad type B. This terrorist cell also consists of three members, but unlike *Triad type A*, all terrorists communicate directly with each other. The relationships built can be either based on live contact or based entirely on online communication. In *Triad type B*, the probability of forming a prominent leadership within the group is highest. The activities of this type of triad are most vulnerable to being intercepted by law enforcement agencies.

In cases where radicalization is achieved in a family environment and the planning, preparation and organization of the terrorist act is carried out by parents and their children (family terrorism) (Ivanov 2024), the nuclear family can be seen as a small terrorist cell.
Small independent terrorist organizational units could be defined as pursuing tactical objectives which they seek to achieve through asymmetric "spatial, temporal or procedural advantage" (Nistorescu 2024).

Regarding the preferred tactical methods for carrying out a terrorist act by "lone wolves" and small self-organized terrorist cells, the most used are edged weapons and firearms, vehicle-ramming attacks, and simple improvised explosive devices (based on gas cylinders).

It should be noted that terrorist acts committed by "lone wolves" professing far-right ideology are characterized by a greater degree of deliberate cruelty, better planning

and preferred use of firearms and improvised explosive devices, while "lone wolves", supporters of Islamist causes, rely on attacks of "convenience" with the use of edged weapons.

Sources and methods of financing "lone wolves" and small terrorist cells

The process of financing terrorism involves the use of various sources and methods of financing, which serve the raising and transfer of financial and material assets and are used both for the perpetration of specific terrorist acts and for supporting activities. They depend on a number of factors such as the size of the terrorist organizational unit, the geographical location of the territory in which the terrorists operate, the degree of adoption of high technologies, measures imposed by states to counter the financing of terrorism, the ethno-cultural origin of the terrorists, levels of the grey and criminal economy, etc.

In 2014, a study was conducted by the Norwegian Defence Research Establishment (FFI) on the most common sources of financing terrorist activity in Europe over the past ten years. The results show that personal funds account for the largest share, followed by robberies and thefts, and in third place is the trade in illegal goods (drugs, weapons, stolen cars, etc.), with amounts in the range of $1,000–$10,000 most often needed to carry out a terrorist attack (Oftedal 2015).

In practice, there is a lack of comprehensive information on the sources and methods of financing "lone wolves" and small self-organized terrorist cells. In Europe, cases of planning, preparation and execution of terrorist attacks by such terrorist structures, which mainly profess far-right or jihadist ideology, have been registered. There are no known acts of terrorism committed by "lone wolves" and small terrorist cells, which are supporters of far-left and ethno-nationalist ideology.

As an observed dependence, it can be pointed out that terrorist attacks planned by far-right terrorists are more resource-intensive, compared to those of Islamists, due to the preferences in the tactical methods used. While very little money is needed to purchase a knife or an axe and they are sold legally, firearms are more expensive and require connections with the criminal contingent, where the price is a matter of speculative agreement.

However, there are isolated cases where "lone wolves" plan a terrorist act that requires the acquisition of larger sums of money. Such is the mass murder committed by the Norwegian far-right terrorist Anders Breivik in July 2011, in which 77 people died and over 300 were injured. The Norwegian used firearms and a van bomb. In his self-written manifesto, Breivik claims that the preparation for the terrorist attack began as early as 2002, and according to initial calculations, about 3.5 million Norwegian

kroner (NOK) were needed (Taylor 2011). These were planned for the acquisition of materials for making explosives, the purchase of handguns and automatic firearms, hand-held anti-tank grenade launchers, ammunition and personal protective equipment, as well as for logistical costs.

The Norwegian used personal funds obtained from salaries and credit cards, legitimate businesses, and the sale of fake university degrees as sources of funding (Normark and Ranstorp 2015). To cover his tracks and legalize the income generated from illegal activities, Breivik created a complex money laundering scheme that included the use of offshore zones in the Caribbean Basin and the subsequent transfer of funds to banks in the Baltic republics and accounts of relatives in Norway (The Dominican 2012).

The case of Anders Breivik is useful for forming scientific knowledge about the financing of "lone wolves" from the far-right spectrum of terrorism, although it does not represent a universal model. The Norwegian used a variety of sources of financing, both legal and illegal. Law enforcement agencies would have a very difficult time intercepting the Scandinavian's fundraising in the initial phase of their accumulation for two reasons – first, the sums of money are of legal origin (personal savings, bank loans and income from legal business), and second, there have been no extremist anti-social acts registered against Breivik that would lead investigators to a reasonable assumption that he was preparing to commit a terrorist act.

When the Norwegian diversified his funding and started trading in fake diplomas, conditions were created for vulnerability and attracting the attention of financial intelligence units. During this period, Breivik committed two illegal acts – making and selling false documents and laundering money. There is then a large cross-border movement of funds, with the ultimate recipient being his mother, after which the amounts are withdrawn in cash. But the money flows still cannot be easily attributed to terrorist financing, as the violent act has neither begun nor been completed.

Breivik used part of the accumulated funds to purchase firearms, and another part to create an agricultural company to cover up the acquisition of large quantities of artificial fertilizers needed to make improvised explosive devices. It is during this stage of preparation for the terrorist attack that the Norwegian's activities can be most easily intercepted on the basis of its financing. There are two key factors – first, a large part of the financial resources are of illegal origin (although laundered), and second, the funds are spent on the purchase of dual-use items, which are supposedly subject to strict state control.

The conclusions of the analysis show that if we consider the process of financing the "lone wolves" as passing through four main stages – *raising funds*, *transferring*, *storing* and *using financial resources* then the financing of terrorist activities can most easily be registered in the *use phase*. Interception is possible in the *transfer* and

storage phases, when terrorists resort to the services of financial institutions and the funds can be blocked by the competent authorities, as long as there are sufficiently justified suspicions that the financial operations serve illegal activity.
The financing of "lone wolves" and small terrorist cells should not be viewed only through the prism of financing a specific terrorist act, but also as raising funds and transferring them to conflict zones to support terrorist fighters and their family members.

The Europol report for 2022 describes several such cases in which "lone wolves" or small terrorist cells organize the raising of funds and their subsequent transfer to prisons and camps in Syria. In one of the cases, it is indicated that in August 2022, a person from the Netherlands transferred more than $ 100,000 to members of the families of the "Islamic State" located in the Syrian refugee camp Al Hol (EUROPOL 2023). Usually, the amounts are raised in the form of donations for campaigns in support of Islamism. They are implemented on various online platforms, including the active use of social networks, the mobile application Telegram and cryptocurrency trading sites. Bank transfers to savings accounts are also being made. Once generated in Europe, the funds are redirected to Syria using the services of so-called "hawaladars", operators of the informal alternative money and value transfer system "hawala".

In October 2023, Italian media reported (Rai - Radiotelevisione Italiana S.p.A 2023) that two individuals of Egyptian origin were arrested in Milan for allegedly conspiring to commit terrorist acts, including online propaganda and threats against Prime Minister Giorgia Meloni. The Egyptians also financed Islamic State terrorists in Syria and Yemen, as well as the families of Palestinian terrorists, through an online fundraising campaign. The Islamists used the platforms of Facebook, Telegram and WhatsApp.

The above-described case reveals the involvement of a small terrorist cell of the *Dyad type* in the financing of terrorism, with the financing being carried out with personal funds through a donation campaign through fundraising accounts.
As a rule, if there is a transfer of funds outside the terrorist *dyad* or *triad*, it is more vulnerable to observation and interception by law enforcement agencies, since it goes beyond the isolated environment of the small terrorist cell, whose members may not have shown any involvement in terrorist activity and have not come into the radar of the security services.

The studied few cases and the assessment made by FATF (Financial Action Task Force) (FATF 2015) show that "lone wolves" and small terrorist cells prefer the use of legal sources for financing terrorism over illegal ones, with the most used being financing with personal funds, legal business and crowdfunding. Less common cases of raising funds of illegal origin are related to fraud and document falsification. There are few known cases of financing with money obtained from thefts and robberies, as well as drug distribution.

"Lone wolves" and small terrorist cells use almost the entire spectrum of methods for financing terrorism, with the formal financial system, digital currency platforms and physical cash transfers being the main ones. It is characteristic that large amounts are rarely transferred, which makes them difficult to detect by the competent authorities.

Possible measures against the financing of small independent terrorist organizational units

Countering the financing of "lone wolves" and small terrorist cells poses a serious challenge to law enforcement agencies in European countries. Although effective mechanisms for countering the financing of terrorism have already been established, both at the international and European levels, the dynamics of the modern security environment require the implementation of specialized approaches to prevent and disrupt the financing of small independent terrorist organizational units.

The proposed measures against the financing of "lone wolves" and small terrorist cells focus on the areas of *prevention* and *disruption*, as this is where the effect would be greatest, due to the specifics of the financing process of the terrorist organizational units under consideration – decentralized financing, mostly small amounts of money, low frequency of transfers, predominant legal sources of financing.
The most appropriate approach would be to cut off their financing at the *stages of storage and use* of the generated funds, since in the *phases of raising and transfer*, proving the relevance of financial assets to activities related to terrorist financing would be more difficult and complicated.

Based on the general theoretical knowledge in the field of countering terrorist financing and based on the researched sources and methods of financing "lone wolves" and small terrorist cells, the following measures can be systematized and proposed:

1. Change and unify the frequency of conducting a *national money laundering and terrorist financing risk assessment* in all national jurisdictions within the European Union (EU). A *national money laundering and terrorist financing risk assessment* in all EU Member States should be conducted once a year.
2. Establish a structural unit within the planned new European Union authority for anti-money laundering and countering the financing of terrorism, which would be committed to countering the financing of "lone wolves" and small terrorist cells. The establishment of the new EU authority is set as a legislative initiative in 2021 and is expected to start operating in 2026 (European Commission 2021).
3. Use specialized research centres to create risky financial profiles of individuals who have been implicated in terrorist activities, and who can be defined as a "lone wolf" or a member of a small terrorist cell.
4. Block the financial assets of individuals who systematically participate in anti-social activities related to acts of violence on racial, ethnic or religious grounds.

5. Create algorithms and use artificial intelligence capabilities for analysing risky online payments for the purchase of dual-use goods or individual components, which together can be used to produce improvised explosive devices, chemical or biological weapons, and homemade combat drones.
6. Create algorithms and use artificial intelligence capabilities for analysing risky online fundraising campaigns for charitable or humanitarian purposes, which can be exploited to finance terrorist activities.
7. Develop legislative and technical mechanisms for financial auditing for the parents of radicalized minors or underage persons.
8. Ensure the adoption of a national program for training local authorities and territorial divisions of regulatory, control, supervisory and specialized bodies on the implementation of measures against the financing of terrorism.
9. Conduct targeted training with the middle management echelon of large companies in the Fintech sector on the sources and methods of financing terrorism and their countering.
10. Conduct targeted training with the leaders of local religious communities on radicalization, terrorism and the sources and methods of its financing.
11. Establish a working group within the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism – MONEYVAL, which will assess the risks and prepare recommendations for countering the financing of "lone wolves" and small terrorist cells on the territory of Europe.
12. Increase penalties for theft of explosives, weapons and ammunition, their illegal storage and transportation, as well as illegal trade.

All proposed measures against the financing of "lone wolves" and small terrorist cells should be considered collectively and in an interrelated manner. They do not provide a definitive solution to the problems under consideration but outline guidelines for improving the overall system for countering terrorist financing.

Conclusions

While years ago, the main threat to Europe's security was considered to be terrorism bombing targeting critical infrastructure, the last decade has proven that acts of terror are not necessarily associated with complex planning and preparation, large-scale financing and skilled operational leadership by an established terrorist group. Attacks carried out by "lone wolves" have a high psychological and social impact, as they demonstrate the vulnerability of social systems. They are difficult to predict, asymmetric, and often fall outside the radar of public order and security services.
In the future, we will probably witness the evolution of "lone wolves" and small terrorist cells, they will acquire higher levels of organization and preparation, and their attacks will become more precise and deadly with the use of diverse tactical methods and the integration of high technologies.

It is also possible that more illegal sources of funding might be included in the portfolio of small independent terrorist organizational units, as well as collaboration with organized crime.

Countering the financing of "lone wolves" and small terrorist cells requires the implementation of a systemic approach, with good cooperation between all entities in the system of countering the financing of terrorism – state institutions and authorities, representatives of the private sector and civil society – being of key importance. Measures against the financing of small independent terrorist organizational units should be considered as part of the general combat against radicalization and terrorism and should achieve a cumulative effect.

References

Al Jazeera. 2024. "Israeli football fans clash with protesters in Amsterdam." https://www.aljazeera.com/news/2024/11/8/israeli-football-fans-clash-with-protesters-in-amsterdam.

Amalaraj, P. 2024. "At least four police hurt in Hague riots after rival Eritrean mobs torched cars, trashed buildings and hurled bricks at cops - turning Dutch city into a war zone." *Daily Mail.* https://www.dailymail.co.uk/news/article-13097091/Hague-riots-broke-violent-clashes-rival-groups-Eritreans-scenes-saw-police-cars-torched-thugs-throw-rocks-Dutch-cops-use-teargas.html.

Anadolu Agency. 2024. "PKK operates freely in Belgium though listed as terror group." https://www.aa.com.tr/en/europe/pkk-operates-freely-in-belgium-though-listed-as-terror-group/3175695.

Bakker, E., and B. de Graaf. 2010. *Lone Wolves. How to Prevent This Phenomenon?* Expert Meeting Paper, ICCT International Centre for Counter-Terrorism - The Hague. https://www.icct.nl/sites/default/files/2023-02/ICCT-Bakker-deGraaf-EM-Paper-Lone-Wolves.pdf.

CTED. 2024. "Evolving Trends in the Financing of Foreign Terrorist Fighters' Activity: 2014 – 2024." CTED Trends Tracker. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_trends_tracker_evolving_trends_in_the_financing_of_foreign_terrorist_fighters_activity_2014_-_2024.pdf.

European Commission. 2021. "Anti-money laundering and countering the financing of terrorism legislative package." https://finance.ec.europa.eu/publications/anti-money-laundering-and-countering-financing-terrorism-legislative-package_en.

EUROPOL. 2023. "EU Terrorism Situation & Trend Report (TE-SAT)." 20. https://www.europol.europa.eu/publications-events/main-reports/tesat-report.

EUROPOL. 2019, 2020, 2021, 2022, 2023. "EU Terrorism Situation & Trend Report (TE-SAT)." Main reports. https://www.europol.europa.eu/publications-events/main-reports/tesat-report.

FATF. 2015. "Emerging Terrorist Financing Risks." Paris. www.fatf-gafi.org/publications/methodsandtrends/documents/emerging-terrorist-financing-risks.html.

Hamm, M., and R. Spaaij. 2015. *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies.* FINAL SUMMARY OVERVIEW, U.S. Department of Justice. https://www.ojp.gov/pdffiles1/nij/grants/248691.pdf.

Ivanov, D. 2024. "The Nuclear family in Modern terrorism." *15th International Scientific and Practical Conference. Environment. Technology. Resources.* Rezekne, Latvia: Rezekne Academy of Technologies. 121-124.

Keatinge, T., and F. Keen. 2017. *Lone-Actor and Small Cell Terrorist Attacks. A New Front in Counter-Terrorist Finance.* RUSI Occasional Paper, 7. Accessed January 11, 2024. https://static.stage.rusi.institute/201701_op_lone-actor_and_small_cell_terrorist_attacks.1.pdf.

Marinov, P. 2022. "Preventing radicalism, anarchism and ultra nationalism." Edited by H Yalçınkaya. *Good practices in counter terrorism* (Centre of Excellence Defence Against Terrorism) 2: 147-163.

Nance, M. 2016. *Defeating ISIS: Who They Are, How They Fight, What They Believe.* Skyhorse Publishing.

Nistorescu, C. V. 2024. "The Asymmetries Generated by New Weapon Systems and Their Role in Achieving Success on the Battlefield. The Impact of HIMARS on the Conflict in Ukraine." *Bulletin of "Carol" National Defence University* 13(3): 117–128. doi:https://doi.org/10.53477/2284-9378-24-34.

Normark, M., and M. Ranstorp. 2015. *Understanding Terrorist Finance. Modus Operandi and National CTF-Regimes.* Swedish Defence University, 10-11.

Oftedal, E. 2015. *The financing of jihadi terrorist cells in Europe.* Norwegian Defence Research Establishment (FFI), 16.

Rai - Radiotelevisione Italiana S.p.A. 2023. "Terrorismo. Due arresti a Milano: "Proselitismo e soldi a Isis". Tajani: "Non c'è rischio imminente"." https://www.rainews.it/articoli/2023/10/terrorismo-arrestate-due-persone-a-milano-blitz-della-polizia-6eaa1096-e2e7-44a6-a695-b427e92c943f.html.

Research Centre for Extremism and Terrorism. 2023, 2024. *Bulletin.* https://rcetbg.com/biuletin/.

Taylor, M. 2011. "Norway gunman claims he had nine-year plan to finance attacks." *The Guardian.* https://www.theguardian.com/world/2011/jul/25/norway-gunman-attack-funding-claim.

The Dominican. 2012. "Norway's worst mass murderer held offshore accounts in Dominica." https://thedominican.net/2012/04/mass-murderer-overseas-accounts.html.

U.S. Department of State. 2019, 2020, 2021, 2022. "Country Reports on Terrorism." https://www.state.gov/country-reports-on-terrorism-2/.

ACKNOWLEDGEMENTS

We express our gratitude to Col. Assoc. Prof. Petar Marinov, Ph.D., DSc. for methodological guidance.

FUNDING INFORMATION
This research was financed by the author.

CONFLICT OF INTEREST STATEMENT
The author 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 in the Research Centre for Extremism and Terrorism at https://rcetbg.com/biuletin/

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The Complexity of the Transition in Combat Operations and Potential Solutions to Streamline the Process

LTC Claudiu-Valer NISTORESCU, Ph.D.*

*Command and Staff Faculty, "Carol I" National Defence University, Bucharest, Romania
e-mail: nistorescu_claudiu@yahoo.com

Abstract

The contemporary armed conflicts that have recently taken place in Ukraine, the Gaza Strip, and Nagorno-Karabakh serve to illustrate the inherent difficulties associated with combat operations. Despite the high degree of transparency on the battlefield, the nature of the conflict, characterized by friction, uncertainty, violence, and high lethality, underscores the pivotal role of the human factor. The operational process remains primarily driven by human decision-making, with the constant planning, preparation, execution, and evaluation of military operations shaped by the human decision-making process.

In this context, the transition during combat operations is identified as one of the most challenging processes, particularly when unanticipated. The lessons learned from past conflicts indicate that the inherent risks associated with a period of change, the mental pressure, and the increased possibility of experiencing a decisive defeat have a multidimensional impact on both the decision-making process and the execution of the operation. In light of the sensitivity of the transition in combat operations, the analysis seeks to identify the principal vulnerabilities and risks inherent to the process, the triggers and indicators that signal its necessity, as well as a series of solutions to enhance its efficiency. The scientific approach is qualitative and empirically oriented, with a focus on examining the impact of new technologies and weapon systems on the conduct of combat operations.

Keywords:

combat operations; transition; culmination point; tactical opportunity; position of advantage.

Article info

Received: 11 October 2024; Revised: 1 November 2024; Accepted: 2 December 2024; Available online: 17 January 2025

Citation: Nistorescu, C.V. 2024. "The Complexity of the Transition in Combat Operations and Potential Solutions to Streamline the Process". *Bulletin of "Carol I" National Defence University*, 13(4): 152-168. https://doi.org/10.53477/2284-9378-24-55

The literature and studies on combat operations indicate that one of the most challenging aspects is the transition from one form of combat to another. This has a direct impact on the balance between offensive and defensive capabilities at the force level (Jones, Palmer and Bermudez Jr. 2023). Nearly 500 years ago, Machiavelli, in his work The Prince, underlined this difficulty by stating that "there is no subject more delicate, more dangerous or uncertain of success, than the orientation of a leader towards change" (Machiavelli 2012, 55). The statement remains pertinent in the present era concerning the capacity of leaders to acknowledge the necessity for transformation and their capability to direct subordinate entities toward a productive transition from one combat scenario to another. The inherent ambiguity of armed combat, its potential for opportunity or chance, or conversely, its lack thereof, frequently necessitates a transformation in its manifestation. Transition at the level of specific armed combat operations may result from the implementation of the operation plan and be based on a decision for execution. Alternatively, it may be imposed by unforeseen changes in the operational situation, in which case it is based on a decision to adjust the operation. Therefore, this activity can be undertaken either for the purpose of exploiting tactical opportunities or due to the insufficient combat capability of the own forces. The initial theoretical approaches to the concept emerged during the interwar period and were further developed by the German army. In accordance with the dialectical relationship between defense and offense, as elucidated by Clausewitz in his treatise on military strategy, the German army, in one of its combat manuals, underscored the importance of the fact that *"unpredictable situations in battle often require a change of operation type. The switch from attack to defense may occur when it is necessary to consolidate gains or when the enemy is exerting great pressure on friendly forces."* (Finkel 2011, 77). In the context of military operations, the term "transition" is used to describe a change in the way armed combat is conducted. This change is often forced upon the military forces involved and is frequently carried out in a violent manner. Such circumstances give rise to feelings of frustration and friction within the context of military operations, necessitating the prompt formulation of decisions and the realignment of combat strategies and techniques. Furthermore, if the commander is unaware of the necessity for transition and it is not executed in a timely manner, the consequences can be catastrophic for subordinate forces.

The description of transition as a concept is not treated comprehensively in the Allied doctrine. Yet, *the Doctrine for land forces operations - AJP 3-2* underlines the fact that *„forces need to be capable of executing rapid transition within the entire range of operations and tactical operations and, also, to exploit the information environment in order to gain a superior position"* (Allied Joint Publication, AJP-3.2 2022, A-V). In conclusion, it can be stated that the transition implies change not only in the combat operations theme but also in the campaign themes. *The Tactics Manual for Land Forces Operations - ATP 3.2.1 identifies the need for tactical forces to "transition rapidly from one tactical activity to another in order to accomplish their stated objectives"* (Allied Tactical Publication, ATP-3.2.1 2022, 1-7). The same publication emphasizes

that the "commander and his subordinates must be mentally and physically prepared to make a rapid transition between offense, defense and enabling operations" (Allied Tactical Publication, ATP-3.2.1 2022, 1-14). United States Army doctrine emphasizes that *"a transition occurs when a commander assesses that units must change their focus from one element of decisive action to another"* (Department of the Army, ADP 3-90 2019, 3-18).

In accordance with doctrinal regulations and combat manuals, the necessity for transition arises for a multitude of reasons, and not merely as a direct consequence of the conclusion of the operation or due to a transient setback. Therefore, transition is an inherent aspect of the conduct of mission accomplishment activities, entailing either a change in the form of combat or a shift from combat to stability operations. Transitions can be challenging, particularly if unanticipated. Therefore, during planning, commanders, with the support of the general staff, identify potential transition scenarios and the indicators that signal the necessity for such transitions. This approach helps to mitigate friction and streamline the adaptation process. Specialized studies have identified the following scenarios where the transition occurs in military operations (www.globalsecurity.org 2003):

1. The transition from combat operations (offensive and defensive) to stability operations entails the achievement of set objectives and the desired end state, the cessation of combat operations, and the gradual transfer of responsibility to government authorities.
2. The transition during combat operations from offensive to defensive tactical operations and actions, and vice versa, includes a number of intermediate operations.

The analysis focuses on the second situation, yielding insights into the transition process at the operational level. These insights are particularly beneficial in the context of a large-scale and intense conventional conflict in the vicinity of Romania's borders. The primary objective of the present study is to identify potential solutions for streamlining the process. Subsequently, research efforts have been focused on identifying the triggering factors of the transition, describing the role of its main components and their impact on the mechanisms of realization of the process, as well as the indicators that warn of a potential situation that requires the realization of the transition. In this regard, the evaluation encompassed an assessment of the transition from a defensive to an offensive stance and vice versa.

In order to direct and guide our research, we have identified a series of key questions that we intend to address:

- What are the situations when a tactical ground force is forced to resort to transition during the conduct of armed combat?
- What are the components of transition, and what is their impact on its onset?
- What are the indicators that signal the imminent culmination of a military force (proximity of its reaching its climax) in an offensive operation?

• What are the warning indicators of the culmination of a military force (proximity of its reaching its climax) in a defensive operation?
• What measures might be taken to facilitate the transition process?

The provision of answers to these research questions contributes to the construction of a comprehensive picture of the fundamentals and mechanisms of transition in combat operations. The intrinsic complexity of armed combat precludes the possibility of conducting an exhaustive analysis of the subject. Nevertheless, the findings may prove beneficial for military commanders and leaders, as well as specialists and theorists in this field.

Situations requiring transition during combat operations

The execution of a transition during a combat operation is a high-risk activity that requires the careful synchronization of all available capabilities and actions. Transition from one form of combat to another is achieved either when the force engaged in a particular type of operation is no longer capable of sustaining it, or when, due to a position of relative advantage, its own forces are in a position to assume the initiative. In this regard, the remarks of the English General Rupert Smith are edifying. In his work The Utility of Force, Smith emphasized that the essence of all tactics and maneuvers, and in general the greatest tactical dilemma, is striking a balance between how much effort to expend in striking the enemy in order to achieve offensive objectives and how much effort to concentrate on countering his retaliation (Smith 2019, 14). By this, he emphasizes the importance and necessity of maintaining a balance between offensive and defensive capabilities to ensure success and avoid defeat. Accordingly, in tactical combat operations, the following situations can be identified in which military commanders must resort to transition:

➢ on the offensive, when own forces can no longer sustain the ongoing operation and continue action on the main lines of advance;
➢ on the offensive, when own forces are forced to consolidate their gains or to take an operational pause with a view to resuming offensive operations at a later date;
➢ in defense, when own forces are in a position of advantage and can seize the initiative, taking offensive action on an enemy who can no longer conduct defensive operations in a cohesive manner by withdrawing;
➢ in defense, when own forces can no longer conduct an effective defense and are forced to withdraw. In each of the aforementioned situations, the transition is based on a sum of factors that relate to the operational situation of combatant parties.

It can be reasonably deduced that the realization of a position of advantage for one of the combatants is directly or indirectly linked to the existence of a vulnerability or even a failure of the opponent. In conclusion, the initiation of the transition is

contingent upon the specific factors inherent to each situation and hinges upon the capacity of one of the parties to accurately discern the indicators that signal a potential shift in circumstances.

Components of transition and their impact on the realization of the process

Transition in combat operations is not only physical but also mental. Furthermore, commanders must initially be aware of the necessity to transition from one form of combat to another, accept the new situation, and assume risks. Once the new situation is understood and the mental acceptance of the need for change has occurred, the commander can then trigger the transition to the physical level by making the decision to do so (Baillergeon 2019, 176). The aforementioned components serve to differentiate the transition process into two discrete phases, which are nevertheless interrelated.

a. The mental component of transition

In the initial phase of the change, the mental aspect is predominant, with the commander acting as the primary catalyst. Subsequent to a comprehensive evaluation of the circumstances and a comparison of his own capabilities with those of the adversary, the commander determines and initiates the transition. Additionally, during this phase, the staff, in accordance with the commander's guidance, initiates the planning of a new operation. The initiation of a new planning process transmits the requisite signals to subordinates, thereby engendering a mental realization of the change. The underlying factors that precipitate the decision to alter the form of combat are the tactical opportunity on the battlefield and the culmination of the operation.

In the absence of a clearly defined opportunity, the decision-making process becomes inherently tactical in nature. United States Army doctrine places significant emphasis on the interconnection between tactical opportunity and the existence of a position of relative advantage. In this context, tactical opportunity can be defined as *"a location or the establishment of a favorable condition within the area of operations that provides the commander with temporary freedom of action to enhance combat power over an enemy or influence the enemy to accept risk and move to a position of disadvantage."* (Department of the Army, ADP 3-0 2019, 4-5). In consequence, the concept of tactical opportunity is transient and predicates the existence of a favorable situation in time and space that can be exploited to strike the enemy's vulnerabilities and subsequently achieve success. In the context of tactical operations, a position of advantage may manifest in a number of ways (Department of the Army, FM 3-0 2017, 1-18):

- In terms of **physical and geographical factors**, this can include the positioning of friendly maneuver forces in relation to those of the enemy, the

maintenance of key terrain, and the control of rear areas;
• In terms of **temporal factors**, this can include staying ahead of the enemy in the decision-making cycle, operational tempo, the speed of the information process, and the effectiveness of the sensor-to-shooter relationship;
• In terms of **freedom of action**, this encompasses the security of lines of communication, the opportunity to exploit friendly forces' striking capabilities beyond the range of the enemy's weapons, the protection of rear areas, and the creation of an A2AD system;
• **Morale and will to fight** – legitimacy of the cause, effective leadership, rational allocation of resources, equipping with high-performance weapons systems, high level of training and interoperability, etc.;
• Achieving **superior combat power** – resulting from an extended range, accuracy, and lethality of weapons systems, concentration of forces, or misleading the enemy.

Tactical opportunities may arise in both offensive and defensive operations. It arises in the context of combat, characterized by uncertainty, ambiguity, and chaos, and may result from the actions of one's own forces or those of the enemy. The capacity to capitalize on opportunities is contingent upon the flexibility and autonomy of thought, initiative, velocity, and audacity exhibited by the commander and subordinate commanders. The initiation and implementation of an action with the objective of exploiting a potential opportunity is an undertaking that entails an inherent degree of risk. It is incumbent upon the commander of the tactical formation to be engaged in combat, as well as his higher, to assume these risks in a deliberated and calculated manner. An adequate allocation of resources and the qualitative superiority of equipment facilitate the commander's willingness to assume risks.

The exploitation of one tactical opportunity usually generates other tactical opportunities that can "create new courses of action or point to new directions to exploit in achieving the higher echelon's objective sooner or with less effort" (Statul Major al Forțelor Terestre, FT 2 2019, 95). In general, the potential for opportunity is linked to the conduct of offensive tactical operations and is contingent upon the capacity of friendly forces to retain the initiative. However, the possibility of capitalizing on an opportunity may also present itself in a defensive context. The successful execution of a counter-attack at the optimal time and location, the extrication of one's forces from an unfavorable situation, and the prevention of the defeat or destruction of one's forces are all contingent upon the exploitation of a tactical opportunity.

The Operation Culmination Point, the second determinant of transition, is the point at which a force can no longer successfully continue the operation in which it is engaged (Allied Joint Publication, AJP-5 2019, 3-12) and must change the form of combat (Department of the Army, ADP 3-0 2019, 2-9). Usually, the climax is

associated with the offensive operation, but it also applies to the defensive operation (Friedman 2017, 105). Therefore, the concept must be approached from the perspective of both the attacker and the defender (Weiss 2021, 263). Thus, in tactical offensive operations, a force reaches its culmination when it can no longer sustain the offensive operation and must switch to defense to avoid defeat. Concurrently, in the efficacy of a defensive tactical operation, a force reaches its climax (culmination point) when it is no longer able to defend itself successfully and create the conditions for a transition to the counter-offensive. In such a situation, in order to avoid defeat, the defending force must be reinforced, relieved, or engaged in withdrawal operations.

By analyzing these two contexts in which a tactical force can experience the climax, we identify, punctually, the main causes that determine this situation.

TABLE NO. 1

Culmination factors in combat operations

DURING OFFENSIVE TACTICAL OPERATIONS	DURING DEFENSIVE TACTICAL OPERATIONS
It no longer achieves greater combat power than the defending force	It no longer has the combat power to stop the enemy's offensive
It no longer has forces to be brought forward to develop the offensive operation, thus losing the initiative.	It cannot mount a cohesive defense
It can no longer logistically support the continuation of the attack	It is in a situation of being overwhelmed by the enemy forces on the offensive

In particular, in the context of combat operations, tactical forces may encounter one or more factors that contribute to the culmination of the operation, either concurrently or sequentially. In any given situation, the role of the commander is of paramount importance in the assessment of the risk and likelihood of culmination by subordinate forces. This will facilitate the transition process considerably. Otherwise, failure to identify this risk in a timely manner will result in an improper transition, with severe consequences for the tactical force engaged in the operation. To illustrate this, if the commander of a tactical formation engaged in offensive operations fails to recognize in a timely manner the significant constraints associated with the introduction of new forces into the fray, this could potentially result in a vulnerability. This vulnerability can be exploited by the enemy once it is recognized that the deployment of forces has reached its culmination. The enemy's counterattack has the potential to catch the formation forces off-guard in a position and location that is disadvantageous to repel it. The commander, based on the information at his disposal and the analyses and estimates provided by the staff, also discerns, in time and space, the possibility that the enemy will reach its culmination. It is therefore possible to conclude that determining this fact can be a valuable opportunity, providing the preconditions for the own forces to take the initiative and subsequently achieve success. A lack of awareness or indecision may result in the failure to capitalize on an opportunity to launch an attack on the enemy when they are at a disadvantage.

By analyzing the fundamentals of combat operations and their main stages, it is possible to determine a number of indicators that are highlighted when a tactical

force reaches or is about to reach the climax of an operation. The following is a list of these indicators and possible actions to be taken in their occurrence, both to avoid the climax and to exploit opportunities. It should be noted that the list is not exhaustive and that an adaptive and intelligent enemy will seek to conceal these indicators.

TABLE NO. 2

Indicators of the culmination point in offensive operations

INDICATOR	ACTIONS
Obtaining information on the initiation of defensive actions: consolidation of seized objectives, retreat on favorable alignments, expansion of combat disposal for the first echelon	Fire and maneuver interdiction of consolidation actions
Drastic reduction in the tempo of offensive actions	Destroying the coherence of the offensive operation by selectively striking command and control elements
Insufficient concentration of forces during attacks on the main offensive directions	Prohibiting the enemy from dislodging forces from other areas of operations
Capture of a large number of prisoners from the offensive force or own assessments of high enemy casualty rate on the battlefield	Intensifying the defense effort to increase the intensity of strikes in affected areas of operations
Indicators of lack of synchronization of combat functions in the enemy's attacks	Executing precise strikes that fragment the coherence of the enemy's combat operations
Identification in the operation area of the first echelon of forces whose destination was known to be part of the reserve	Identifying options for the possibility of changing the type of operation by own forces
Interception of lines of communication by own forces and blocking the logistical flow to enemy first echelon units	Deployment of forces and weapon systems, both to protect your friendly forces' flanks and also to conduct a possible encirclement of the enemy
The discovery by defending forces of a large quantity of abandoned combat equipment and techniques.	Intensification of strikes on the enemy and preparations for the change of the operation type

TABLE NO. 3

Indicators of the culmination point in defensive operations

INDICATOR	ACTIONS
Information and reports on enemy force penetrations into the ZO of neighboring units	Requests for information/clarification from higher echelons and on the need to redeploy own forces, including principal weapon systems
Information and reports of enemy capture and occupation of key points in the enemy's own forces' rear area	Rapid deployment of reserves to counter these actions
Reports of low morale and obvious physical and mental exhaustion of soldiers	Staggered replacements of forces, countering enemy undermining of the will to fight
Neutralization of artillery and air defense missile systems of own forces;	Redeployment of available weapon systems, request for support from higher echelon.
Drastic reduction in the PL of second echelon units intended for counterattack	Requesting support from higher echelon for replenishment of reserves
Commitment of second echelon or reserves, followed by the impossibility of their regeneration or replacement	Awareness of the culmination and request for withdrawal
Striking and destruction of the logistic system	
Significant increase in casualties from enemy attacks	Requests for replacements of forces and weapon systems
Clues and information about concentrations of superior forces of the attacker on the main offensive directions	Repositioning of forces and main weapon systems

These indicators are determined by the staff as part of the operation planning process and fall within the *Commander's Critical Information Requirements/CCI)* which is that "information requirement identified by the commander and staff as essential to facilitate timely decision-making" (Statul Major al Forțelor Terestre, FT 2 2019, 22). Specifically, these indicators underpin *Friendly Forces Information Requests/FFIR)* and *Essential Enemy Friendly Information/EEFI*. FFIR is the information that the commander needs to know about the situation of his own forces, and EEFI is

the information that needs to be concealed from the enemy. Once established in the planning process, the indicators must be continuously monitored in order to provide the commander with situational awareness, including the proximity of the culmination of friendly forces. Finally, it is imperative that the commander and their staff consider the possibility that the enemy may be engaging in misleading operations and that certain culmination indicators may not accurately reflect the operational status of enemy capabilities. Therefore, an imperative of the operational process carried out by friendly forces is *to develop "effective procedures to counter the deceptive actions carried out by their adversaries, so that the achievement of their own mission is not jeopardized"* (Toroi and Stanciu 2023).

It is indubitable that the identification and exploitation of tactical opportunities on the battlefield can engender success. Furthermore, determining the enemy's culmination point and identifying the increased risk of reaching one's own culmination point can also be pivotal in determining the outcome of a battle, with victory or defeat being the potential results. The examples from the past are not few and emphasize that "one of the most difficult things for a commander is to admit defeat or in other words the inability to achieve success." (Baillergeon 2019, 181). This is particularly the case for a commander who is on the offensive and who will experience significant psychological challenges in accepting the unfeasibility of achieving the initial objectives. In the winter of 1994, the commanders of the Russian forces engaged in the assault on Grozny demonstrated a lack of awareness of the inherent risks and did not accept the impossibility of conquering the city. Frustration and ignoring the indicators of the climax led to the disaster of the Russian mechanized forces: "*in a few hours, the Russian units were blocked in the streets, their armor destroyed by the enemy, who was firing freely from the roofs of the buildings and from the cellars, positions that could not be neutralized by tanks*". (Oliker 2001, 13). After more than twenty years, the Institute for the Study of War (ISW), in one of its analyses of the unfolding conflict in Ukraine, emphasized that "*the initial phase of the Russian campaign in Ukraine was effectively repelled by Ukrainian forces. The campaign, which sought to seize control of major Ukrainian cities including Kiev, Kharkov, and Odessa through a series of mechanized and airborne operations, ultimately proved unsuccessful in its objective of forcing a change of government. The offensive operation has reached its culmination (at the time of writing). Despite achieving minor successes, it seems unlikely that Russian forces will be able to achieve their original objectives through this method.*" (Kagan, Barros and Stepanenko 2022). In a subsequent study published by the same research institute, the causes of the cessation of the Russian offensive in the Kiev area were investigated. One of the most significant indicators identified was the undertaking of defence-specific actions, including the planting of minefields (Kagan 2022). Concurrently, several months later, Russian troops were able to evade encirclement at Izyum and avert a catastrophic defeat when they were caught by the Ukrainian counteroffensive in Kharkiv (Kofman and Evans 2022). A similar situation occurred in the Herson area of operations, where the Russian forces were withdrawn to the left bank of the Dnieper. At that time, the advantage of the Ukrainian forces was difficult to challenge (Hird et al. 2022).

The culmination of the operation and the tactical opportunity are inextricably linked in terms of both temporal and spatial considerations. They play a significant role in initiating the transition, initially at the mental level and subsequently in action. The manner in which these characteristics of military action are managed has a direct bearing on the outcome of the tactical operation. In this sense, the reaching of the climax by friendly forces represents not only a loss of initiative and a change of the combat form but also an opportunity for the enemy. If the enemy becomes aware of the inevitability of the culmination of the friendly forces, it is likely that he will intensify their efforts to exploit the situation. It is therefore imperative that the commander of the friendly forces prioritize the protection of information regarding this event and the masking of its indicators. Similarly, the enemy's culmination represents an opportunity for its own forces. In conclusion, it is of paramount importance to determine the point at which either our own or enemy forces can reach their climax during the planning process.

b. The physical component of transition

The second key component of the transition is physical and represents the totality of actions taken to prepare and execute the tactical transition from one form of combat to another (Baillergeon 2019, 175). Referring to this component the analysis will consider the transition from offense to defense and the transition from defense to offense, highlighting the main factors that the commander and his staff must consider in order to streamline the process.

➢ *The transition from offense to defense*

The transition from offense to defense is a challenging process, both mentally and physically, as commanders and subordinate forces must adapt their operations and alter the form of combat as initial actions are carried out. The complexity of the transition from offense to defense can be attributed to the interplay of the following factors:

- The necessity to adopt a defensive posture arises when an offensive operation culminated, or alternatively, forestalls the culmination.
- The restructuring of defensive combat disposal is a significant challenge in light of the dispersion of forces.
- Furthermore, it is essential to identify and occupy the terrain in order to facilitate the implementation of a defensive operation.
- Low morale due to a feeling of "defeat" when offensive actions stop.

Military experts and theorists have identified two main methods that allow an offensive force to switch to defense in an algorithmized way (Department of the Army, FM 3-90 2023, 3-12). The initial procedure entails that upon the commander's recognition that the viability of the offensive operation has reached its limit, the forces currently engaged in combat undertake limited offensive actions to secure key terrain on the battlefield that will facilitate the subsequent organization of defensive measures. This method presents a number of advantages and disadvantages. In terms

of advantages, this approach facilitates the establishment of a more robust defensive position, allows for the accumulation of resources to reinforce the main forces, and enables sustained engagement with the adversary. The principal disadvantage is the difficulty of executing limited offensive actions by the forces in contact in order to create a zone of cover. The second method for transitioning from an offensive to a defensive posture entails the organization of the covering area on the alignment where the offensive forces have been halted. This facilitates the backward movement of the main forces, enabling the establishment of a robust defensive alignment on the ground. The principal benefits of this approach are the potential to establish a robust defensive position in the terrain, with the caveat of requiring the deployment of a portion of the forces in an unfamiliar environment. Conversely, the disadvantages of this procedure include a lack of depth and the necessity to coordinate actions when traversing the terrain.

In the situation when friendly forces are on the offensive and the commander realizes that it is nearing its culmination and transition is necessary, he can concentrate the effects of the weapons systems in order to:

- occupy key points in the terrain that will enable him to organize the defenses on a favorable alignment, while giving depth to the combat disposal;
- support the disengagement of forces in contact that no longer have sufficient combat power to break contact;
- strike enemy forces preparing to execute the counter-attack;
- concentrate air defense systems in order to protect friendly forces during relief operations and regrouping;
- concentrate anti-tank systems to stop enemy armored attacks in order to create breaches during the organization of the defense by friendly forces.

In accordance with the circumstances, the commander of the own forces will select one of two procedures, weighing the inherent risks, the capacity of the own forces to execute the transition in an efficacious manner, the support provided by the higher echelon, the nature of the operation to be conducted, and the actions of the enemy.

➢ *The transition from defense to offense*

The shift from a defensive to an offensive operation has been initiated *„by anticipating when and where an enemy force will reach its culminating point or require an operational pause before it can continue.*" (Department of the Army, FM 3-90 2023, 8-24). In order for a defending force to be able to effectively transition to an offensive operation, a number of conditions must be met. These include the enemy having lost the initiative and no longer having sufficient forces to develop operations, the enemy no longer achieving air superiority on the main offensive axes, and the enemy's combat strength no longer being at a higher level than that of the defending force.

The commander of the defending force must act promptly to seize the initiative and exploit the temporary disadvantage of the attacker. The opportunity to undertake an

offensive posture is contingent upon the availability of enemy air defense and anti-armor capabilities on the main operational axes. The establishment of the second echelon and reserves is also a prerequisite for a change of the operation's theme. Once a decision has been made, the commander of the tactical formation has two options for changing the battle posture. The first is to reconfigure the battle disposal, and the second is to relieve the forces and advance with the second echelon (Department of the Army, FM 3-90 2023, 8-25).

Both scenarios possess both advantages and disadvantages, entailing the concentration of forces in specific directions to attain a favorable equilibrium of forces. In such cases, it is often necessary to transfer operational control of specific areas to other forces, or alternatively, to maintain control with a minimal number of forces in order to prevent enemy penetration. The former approach involves the use of forces that are already in contact with the enemy, and offers a number of potential advantages:

- The time required to initiate an offensive maneuver is less than that needed to replace forces already engaged in combat. This allows the opportunity created to be exploited without allowing the enemy sufficient time to consolidate its defenses;
- The process is less complicated because it does not involve coordinating the replacement of forces. This is true whether we are talking about a relief in place or a passage of lines;
- The forces in contact have a better understanding and relationship to the existing tactical situation than forces newly introduced into the fight.

From a human perspective, the forces already in contact have already acquired an understanding of the enemy's tactics and are aware of his strengths and vulnerabilities.

Nevertheless, this approach has inherent disadvantages:

- The concurrent planning and preparation of an offensive operation with the execution of current defensive actions places significant demands on both the general staff and subordinates;
- There is a high risk that the forces in contact will not be in optimal physical and mental condition due to the actions executed up to the moment of going on the offensive;
- It is possible that some of the equipment and weapons systems employed by the forces in contact may be inoperative, and that the forces already in contact may experience logistical difficulties. In such a scenario, it would be prudent to replace essential equipment and weapons, or even to supplement them, and to build up logistical stocks.

The second procedure entails initiating an offensive with forces that are not in direct contact with the enemy. These forces are typically generated by the second echelons of brigade or division-level formations or by units in reserve. This

approach offers several advantages:

- forces not in direct contact with the enemy will be in much better physical and mental condition than those already engaged in the operation;
- forces not engaged in the operation should have no logistical problems;
- the planning of the operation is done out of contact and does not involve the execution and conduct of other operations.

The following disadvantages have been identified:

- The replacement of forces in contact necessitates a longer time to initiate an offensive action;
- Additionally, the concentration of forces along the routes of ingress and egress to and from the contact zone, as well as within the contact zone itself, presents a significant challenge in terms of force coordination. This is further compounded by the heightened risk of enemy identification, particularly of replacements and concentrations of forces;
- Furthermore, in situations where forces are replaced through the process of going into combat, the offensive forces have limited time to connect directly to the existing tactical situation.

In terms of defense, it is typical for the forces in question to lack the initiative and, as a result, must effectively utilize their own weapons systems in order to compel the enemy to fail in their attack. It is therefore incumbent upon commanders to consider the following:

- It is essential to prioritize the neutralization of enemy armored vehicles in the primary axes of advance.
- Furthermore, it is vital to target the second echelon in the rear area and form up places, both during the approach to the contact formation and upon entering combat;
- The strike of the enemy logistic system;
- Anti-aircraft protection was provided for the own forces deployed in the rear area (second echelon). This was done in order to maintain the option of executing a counter-attack and switching to a counter-offensive;
- The implementation of a select number of tactical maneuvers, designed to seize pivotal locations on the battlefield, serves to pave the way for a more expansive and decisive offensive.

In conclusion, regardless of the process chosen by the commander to make the transition from defense to offense, the purpose of the operation, the key tasks, and the end state must be clearly provided to subordinate forces. The commander, supported by his staff, must also consider the following aspects for the execution of the offensive operation: development of the scheme of maneuver, operations in depth to gain control of key points in the terrain, and to weaken the enemy's combat power, security of the flanks and rear area, decisive operation striking the enemy's center of gravity as well as maintaining the capability to develop the offensive, mobility and

counter mobility operations, permanent generation of reserves, judicious allocation of weapons systems to achieve the desired effects on the battlefield.

In conclusion, regardless of the process selected by the commander to facilitate the transition from a defensive to an offensive stance, it is imperative that the purpose of the operation, the key tasks, and the desired end state are clearly communicated to subordinate forces. In addition, the commander, with the assistance of their staff, must consider the following aspects in order to successfully execute an offensive operation: the development of a scheme of maneuver, operations in depth to gain control of key points on the terrain, and to weaken the enemy's combat power, the security of the flanks and rear area, a decisive operation striking the enemy's center of gravity, as well as maintaining the capability to develop the offensive, mobility and counter mobility operations, the permanent generation of reserves, and the judicious allocation of weapons systems to achieve the desired effects on the battlefield.

Conclusions

Armed combat, by its very nature, represents a phenomenon that is unique to the human experience. It is simultaneously shaped by the ever-changing nature of war. The necessity for change and the capacity for transition remain constant features of armed combat. They depend on two factors: the immutable nature of armed combat and the variable character of the phenomenon.

The transition process, comprising both mental and physical components, is widely acknowledged as an inherently delicate phase in the context of armed combat. It is often observed that this phase gives rise to a range of challenging emotions and behaviors, including frustration, friction, and an increased risk of adverse outcomes. In their role as promoters of the operational process, commanders must possess an understanding of the operational context and the effects to be achieved. They must also be able to direct and coordinate the efforts of subordinate forces in order to facilitate an efficient transition process. As the principal decision-maker, he is responsible for initiating the transition, whether driven by the necessity to capitalize on an opportunity or to circumvent a critical juncture. It is therefore evident that the explicit articulation of the commander's intent is a crucial determinant of the success of the transition, whether it entails a shift from a defensive to an offensive posture or vice-versa. Concurrently, in light of the inherent uncertainties and risks associated with a transition in operational posture, it is incumbent upon the commander to cultivate a conducive environment for its realization. Mission command represents an efficacious instrument for conferring upon subordinate commanders the requisite authority and operational autonomy. A command philosophy that is based on mutual trust, professionalism, and the responsibility of subordinate commanders to act in accordance with the intent of the higher echelon is the only one that can create the preconditions for success or avoid defeat.

The analysis, which commenced with a comprehensive literature review and delved into the nuances of armed conflict in the context of evolving trends and technologies in contemporary warfare, has yielded insights that address the research questions. These findings yield a series of insights that can inform the tactical commanders during the operation process, encompassing the planning, preparation, execution, and evaluation phases.

First, by exploring the research directions related to the proposed objectives, we identified potential situations in which the transition may manifest itself at the level of armed combat. The analysis of the main components of transition helped to determine the mechanisms by which the process is realized, while also creating the opportunity to identify options for process improvement. The results of the research indicate that success in the physical (action) component of the transition is directly dependent on how the mental dimension of the process is managed. The research results also emphasize that whether exploiting an opportunity or approaching the climax, the commander's decision is crucial. On it, there depends the ability of subordinate forces to execute the actions necessary for the transition. Consequently, the success or disastrous defeat of one's own forces is influenced by the commander's ability to exploit a position of advantage or to create one when it does not exist. Opportunity comes as a result of the existence, in space and time, of a position of advantage, but at the same time, the avoidance of the climax is influenced by its temporary attainment. From this perspective, it must be realized that in combat those "windows of opportunity", that offer a relative advantage, are limited in time and must be exploited quickly so that the set objectives are achieved.

The identification of culminating indicators provides the commander with the information he needs to make informed decisions during execution, thereby limiting the effects of critical situations and exploiting opportunities. Moreover, these indicators can assist the commander and his staff in the planning process, enabling them to anticipate critical situations or potential opportunities and facilitate an effective transition. The effective employment of weapon systems in the tactical land force formations' equipment can facilitate the transition process. Technological superiority provides the foundation for attaining a relative advantage. Consequently, if the upper echelon possesses qualitatively superior capabilities, including new weapon systems, the formations equipped with them must be allocated to support the forces initiating the transition, irrespective of the circumstances.

It bears reiterating that the transition in combat operations represents a significant challenge and a crucial test for the commander of the tactical structure of land forces. In addition to the tactical and operational implications inherent in this process, there are also civilian issues that must be considered. The influx of refugees, the occurrence of collateral casualties, and the provision of humanitarian assistance impede military operations and, consequently, the transition process. It is thus incumbent upon the commander to give particular attention to both the military and civilian aspects.

Consequently, the potential consequences of military operations, particularly in relation to the deployment of weapons systems, must be continually evaluated in terms of the risk of casualties and collateral damage.

References

Allied Join Publication, AJP-01. 2022. *Allied Joint Doctrine.* Edition F, Version 1. Bruxel: NATO Standardization Office (NSO).

Allied Joint Publication, AJP-3.2. 2022. *Allied Joint Doctrine for Land Operations.* Edition B. Brussels: NATO Standardization Office (NSO).

Allied Joint Publication, AJP-5. 2019. *Allied Joint Doctrine for the Planning of Operations.* Bruxel: NATO Standardization Office (NSO).

Allied Tactical Publication, ATP-3.2.1. 2022. *Allied Land Tactics.* Edition C, Version 1. Brussels: NATO Standardization Office (NSO).

Baillergeon, Frederick A. 2019. *Transitions: Adapting to Change in Division Large-Scale Combat Operations.* Vols. Large-Scale Combat Operations – The Division Fight. US Army Command and General Staff College Press Book, Army University Press.

Department of the Army, ADP 3-0. 2019. *Operations.* US Army.

Department of the Army, ADP 3-90. 2019. Offense and Defense. SUA: US Army.

Department of the Army, FM 3-0. 2017. *Operations.* US Army.

Department of the Army, FM 3-90. 2023. *FM 3-90, Tactics.* US Army.

Finkel, Meir. 2011. *On Flexibility, Recovery from Technological and Doctrinal Surprise on the Battlefield.* Stanford: Stanford University Press.

Friedman, B.A. 2017. *On Tactics: A Theory of Victory in Combat.* Annapolis, Maryland: Naval Institute Press.

Hird, Karolina, Grace Mappes, Kateryna Stepanenko, Madison Williams, Yekaterina Klepanchuk, Nicholas Carl, and Mason Clark. 2022. "Russian Offensive Campaign Assessment, November 9." *Institute for the study of war.* https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-november-9.

Jones, Seth G., Alexander Palmer, and Joseph S. Bermudez Jr. 2023. "Ukraine's Offensive Operations: Shifting the Offense-Defense Balance." *CSIS Brief.*

Kagan, Frederick W. 2022. "What Stalemate Means in Ukraine and Why it Matters." *Institute for the study of war.* Edited by ISW Press. Institute for the Study of War. https://www.understandingwar.org/backgrounder/what-stalemate-means-ukraine-and-why-it-matters.

Kagan, Frederick W., George Barros, and Kateryna Stepanenko. 2022. "Russian Offensive Campaign Assessment, March 19." *Institute for the study of war.* Edited by ISW Press. Institute for the Study of War. https://www.understandingwar.org/backgrounder/russian-offensive-campaign-assessment-march-19.

Kofman, Michael, and Ryan Evans. 2022. "Ukraine's Kharkhiv Operation and the Russian Military's Black Week." *War on the rocks.* War On The Rocks. https://warontherocks.com/2022/09/ukraines-kharkhiv-operation-and-the-russian-militarys-black-week/.

Machiavelli, Niccolo. 2012. *The Prince, Marea Britanie.* London: Amber Books Ltd.

Oliker, Olga. 2001. *Russia's Chechen Wars 1994–2000: Lessons from Urban Combat.* Santa Monica, SUA, California: Arroyo Center, RAND Corporation.

Smith, Rupert. 2019. "The Utility of Force." London: Penguin Books, Penguin Random House.

Statul Major al Forțelor Terestre, FT 2. 2019. *Manualul activității de stat major a comandamentelor din forțele terestre în operații.* București: Statul Major al Forțelor Terestre.

Toroi, George-Ion, and Cristian Octavian Stanciu. 2023. "Sprijinul structurilor de informații în contracararea acțiunilor de inducere în eroare ale adversarului la nivel operativ." *Buletinul Universității Naționale de Apărare Carol I* 12 (2): 142-156.

Weiss, Geoffrey F. 2021. *The New Art of War - The Origins, Theory, and Future of Conflict.* Cambridge: Cambridge University Press.

www.globalsecurity.org. 2003. "Chapter 8: CA Methodology: Transition." *FM 3-05.401 Civil Affairs Tactics, Techniques, and Procedures.* Washington: Department of the Army. https://www.globalsecurity.org/military/library/policy/army/fm/3-05-401/chpt8.htm.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Concept development assessment game – suitable collecting framework in scientific military research

LTC George-Ion TOROI, Ph.D.*

*"Carol I" National Defence University
e-mail: george_toroi@yahoo.com

Abstract

Scientific research is crucial for progress across all areas of society, including the military sphere. However, as the security environment becomes increasingly dynamic, unpredictable, and complex, research methods in military sciences must address contemporary challenges by providing flexible frameworks for evaluating and testing new concepts necessary for the adaptation of force structures. This article analyzes the Concept Development Assessment Game (CDAG), which offers a structured framework for collecting qualitative data in military-specific research. The game serves as a qualitative tool used for testing and refining concepts at an early stage of development, providing a controlled and flexible environment for collecting necessary data. Moreover, it ensures a mechanism for employing a wide range of data collection methods, such as observation, focus groups, or questionnaires, thereby enabling the triangulation of collected data and, consequently, the foundation for valuable outcomes in the effort to transform military structures.

Keywords:
CDAG; military science; collection method; scientific research.

Article info
Received: 12 November 2024; Revised: 29 November 2024; Accepted: 4 December 2024; Available online: 17 January 2025

Citation: Toroi, G.I. 2024. "Concept development assessment game – suitable collecting framework in scientific military research". *Bulletin of "Carol I" National Defence University*, 13(4): 169-183. https://doi.org/10.53477/2284-9378-24-56

In a continuously changing security environment, characterized by intense competition among actors (Joint Doctrine Note 1-19 2019, 1; Mazarr et al. 2018, 1; Mazarr, Blank et al. 2022, 111-113; MCDP 1-4 2020, 1-3), where conflicts and technologies evolve rapidly, the adaptation of forces to current challenges represents an operational necessity to establish the prerequisites for operational success in potential future conflicts (Nistorescu 2024, 195).

In this context, research and conceptual development in the field of military sciences require flexible and innovative methods for testing and evaluation to address these challenges. The Concept Development and Assessment Game (CDAG) emerges as an essential qualitative method, enabling in-depth analysis of theoretical concepts within a controlled environment where operational risks are minimized. CDAG provides researchers with a platform to test complex scenarios, ranging from new doctrines and strategies to emerging technologies and operational procedures, thereby supporting the continuous adaptation of defence structures.

As military sciences rely both on rigorous data collection and the qualitative interpretation of phenomena, CDAG represents an ideal framework for collecting and analyzing relevant qualitative data. Through its exploratory nature, this method allows researchers to capture the nuances and complexity of participants' behaviours and perceptions, thereby creating a solid foundation for understanding and improving the concepts under study.

Research problem

Although there are works addressing aspects of the Concept Development and Assessment Game (CDAG) in a military context, in Romanian literature, in-depth research on this topic remains extremely limited. The lack of systematic approaches represents a significant gap in the Romanian specialized literature, requiring careful investigation to clarify and structure the ways in which CDAG can support military scientific research and provide reliable results in this field.

Research aim

For this reason, the present study aims to provide an in-depth understanding of the correct use of CDAG for data collection, as well as to explore the advantages and limitations of the game as a data collection tool in military scientific research, highlighting its role in the continuous adaptation of doctrine and defence structures.

Research target

This paper is aimed at all researchers in the field of military sciences, especially those at the beginning of their journey. It seeks to provide an adequate, coherent, and valid structural framework for data collection specific to the military domain, as well as viable guidance on the methodological options necessary to ensure the logical coherence of their research when opting for such an instrument.

Research methodology

The methodology employed in this study is a qualitative one, with the goal of understanding and presenting the nuances of the Concept Development Assessment Game (CDAG). The primary method used was document analysis, which enabled an in-depth exploration of the topic and the identification of CDAG's essential elements, thus providing a broad and detailed understanding of the subject.

Given the qualitative nature of the study, the following research questions guided this scientific approach:

- What is CDAG, and how is it conducted?
- What are the benefits and advantages of using CDAG in military sciences research?
- What are the potential limitations of using CDAG, and how can they be mitigated?

Paper structure

The paper is organized into two main sections to address the research questions. The first section focuses on the theoretical presentation of what CDAG is, providing a practical guide for its organization and use to ensure an efficient operational framework. The second section is dedicated to highlighting the main advantages of using this instrument as a framework for data collection in research specific to the military field. It also discusses the primary limitations and considerations that should be taken into account when choosing to employ such a game.

CDAG – what is it and how is it conducted?

The Concept Development Assessment Game (CDAG) is a practical tool, validated by NATO, which provides a framework for refining various conceptual documents within the Alliance. Since the game's name has not been implemented in Romanian, this article will use the terms CDAG and "*Joc pentru dezvoltarea și evaluarea conceptelor*" interchangeably, both referring to the same concept.

NATO specifies that this method can be used to test and refine a wide range of documents, such as doctrines, concepts, policies, manuals, or specific processes, and it has already been employed in major NATO projects (NATO ACT 2014, 2).

CDAG is an analytical wargame developed jointly by NATO's Allied Command Transformation and the Netherlands Ministry of Defence Research Organization (NATO ACT 2011, 12). Generally, wargames are recognized as effective methods for defence experimentation (UK Ministry of Defence 2021a, 58).

CDAG serves as a qualitative method for testing and developing conceptual documents (NATO ACT 2021, 30). While some researchers agree that no universally accepted definition of qualitative research exists (Salmons 2022, 2) and that it is inherently challenging to define (Hennink, Hutter and Bailey 2020, 41), it is widely acknowledged as the most suitable approach when explaining, understanding, or

describing phenomena, processes, or behaviours (Hennink, Hutter and Bailey 2020, 43); (Ravitch and Carl 2021, 49).
Given its exploratory nature, qualitative research allows for conclusive data collection about phenomena, focusing on context, individual perspectives, and the subtleties associated with the subject under study (Salmons 2022, 2; Sharan B. Merriam 2019, 5). For this reason, CDAG's qualitative nature directs researchers' efforts toward studies aimed at understanding phenomena, nuances, or participants' experiences and perspectives regarding the tested concepts.

The nature of research objectives and questions is a critical factor influencing the direction of research and determining whether a qualitative approach is appropriate (Leavy 2023, 9; Leavy 2020, 2). In military-specific research, CDAG as a qualitative method can be used to test how military structures respond to the introduction of new weapon systems or technologies or to evaluate the adaptability of specific defence strategies.

In such cases, the qualitative method enables researchers to gain a detailed understanding of perceptions, team dynamics, and challenges faced by participants, offering profound insights into real behaviours and interactions. Furthermore, the game can serve as a data collection framework for exploring participants' reactions and impressions to a new doctrine or procedure, testing how these integrate into decision-making processes and identifying potential areas for improvement.
Qualitative research in these contexts provides not only feedback on the viability of tested procedures and doctrines but also insights into participants' adaptability. Thus, CDAG becomes an effective qualitative research method in the military field, focusing on obtaining a deep understanding of participants' reactions and perspectives, thereby facilitating the adaptation and refinement of military concepts based on real needs.

The Concept Development Assessment Game is a "tabletop" game focused on resolving scenarios created using the concept card provided. The game's purpose is to test the previously developed concept and identify existing gaps and optimization paths. Therefore, the game is not recommended as an initial step in the research process. Its role is to consolidate an idea or concept developed through other methods and identify solutions to mature the concept further.
Before applying this game, it is recommended to assess its viability. NATO provides guidance on determining the appropriateness of CDAG use based on the maturity level of the concept under analysis and military operations, as illustrated in Figure No. 1.

At a minimum, the Concept Development Assessment Game (CDAG) requires the following participants:

- Game teams
- Analysts

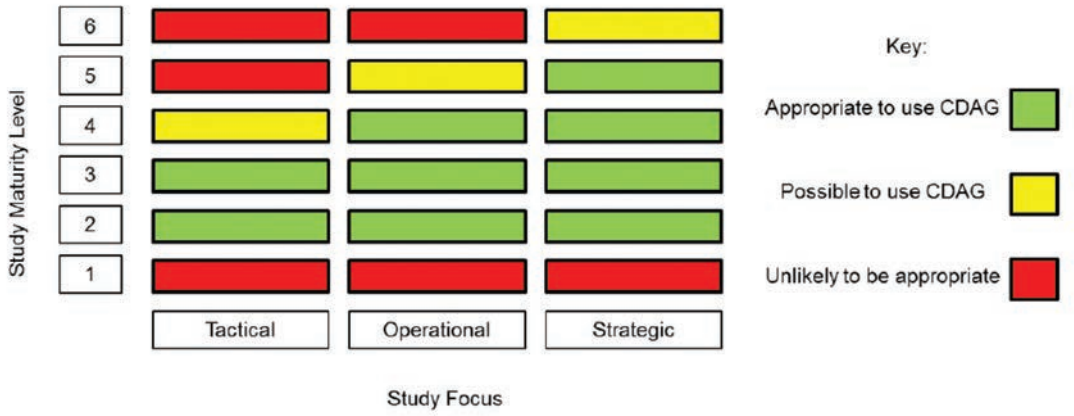


Figure 1 CDAG suitability test
Source: NATO Concept Development Assessment Game "CDAG" Handbook 2014, 6.

- Concept leader/advisor
- Moderator

The game teams are responsible for testing the concept during the game. Unlike adversarial wargames, CDAG is non-competitive; all participating teams have the same responsibilities and work to solve the same problem. There is no upper limit on the number of teams, but a minimum of two teams is required. Each team should consist of 6–8 players with expertise in the specific domain of the concept being tested. Ideally, these players belong to the category of personnel who will regularly operate with the concept if implemented. The teams' primary role is to analyse and critique the concept being tested, adhering to the game's rules to identify vulnerabilities within a concrete scenario.

Analysts play a critical role in data collection, with at least one assigned to each game team. Their function is crucial for the data collection phase of the scientific process. Therefore, a preparatory stage before the game is essential to train analysts. It is recommended that each working team have a dedicated analyst throughout the game. The analyst's responsibilities include monitoring not only the responses provided but also participants' reactions during the game, as well as alternative solutions that may have been discarded during the rounds. Additionally, the data analysis process must consider potential biases from individual analysts. Applying reflexive measures during data collection can help minimize the impact of such biases on the collected data.

The concept leader is the person who developed the concept, document, or product to be tested and refined through CDAG. Their involvement in the game should be kept to a minimum to avoid influencing participants regarding potential solutions. Their role should be limited to clarifying specific aspects of the concept developed if needed by the teams' players.

The moderator is a key element during one of the game's critical stages—the plenary sessions. The moderator guides the discussions between teams to ensure the objectives for each round are achieved. It is recommended that the moderator understand the concept but be someone other than the person who developed it to avoid influencing team discussions.

All these roles are crucial for the potential outcomes of CDAG. Therefore, special attention should be given to the sampling strategy. Considering the qualitative nature of the data and the specific methods of data collection during the game, the sampling should be **non-probabilistic**, most likely subjective, based on predefined criteria (Rassel et al. 2020, 243). This approach involves deliberately selecting the sample rather than choosing randomly (Moser and Korstjens 2018, 11).
This method is a common practice in qualitative research (Dawson 2019, 49); (Hennink, Hutter and Bailey 2020, 164; Braun and Clarke 2013, 55). Predefined selection criteria should include participants' expertise, group homogeneity, or their level of interest in the subject.

CDAG is structured into **six rounds** conducted over a maximum of four days, following the schedule outlined in the table below. Longer durations have proven inefficient due to participants' waning interest and attention.

TABLE NO. 1

Tentative CDAG Schedule

Schedule	Day 1	Day 2	Day 3	Day 4
08.00 – 11.00	❖ Admin activities ❖ Presentations	Round 1	Round 3	Round 5
12.00 – 15.00		Round 2	Round 4	Round 6

The first day must be dedicated to administrative activities for preparing participants and organizing the workspaces. This includes a series of presentations covering the game's methodology and objectives, the employed scenario, the team composition and participant roles, as well as the concept to be tested. These presentations aim to ensure an optimal understanding among participants regarding the game's process and the expectations for its potential outcomes.

Additionally, since one of the methods for collecting data from participants is through a questionnaire (as will be detailed later), it is recommended that the methodology for completing the questionnaire also be explained on the first day to optimize the game.
To ensure the rigour of the game, it is advisable to establish a set of rules to be presented during the administrative activities. These rules should remain visibly displayed in physical format in the workspaces throughout the game.
Moreover, on the first day, it is necessary to allocate workspaces for each team

and provide the necessary logistical support: laptops, flipcharts, markers, pens, highlighters, post-it notes, etc. This ensures an optimal framework for the game to proceed smoothly over the following days.

As mentioned earlier, the Concept Development Assessment Game (CDAG) consists of six rounds, each lasting approximately three hours. These rounds are independent, meaning the results of one round do not influence the activities in subsequent rounds. Each round involves the two-game teams, both performing the same four main phases, as illustrated in Figure no. 2:

- Introductory phase.
- Working phase.
- Plenary phase.
- Round questionnaire.

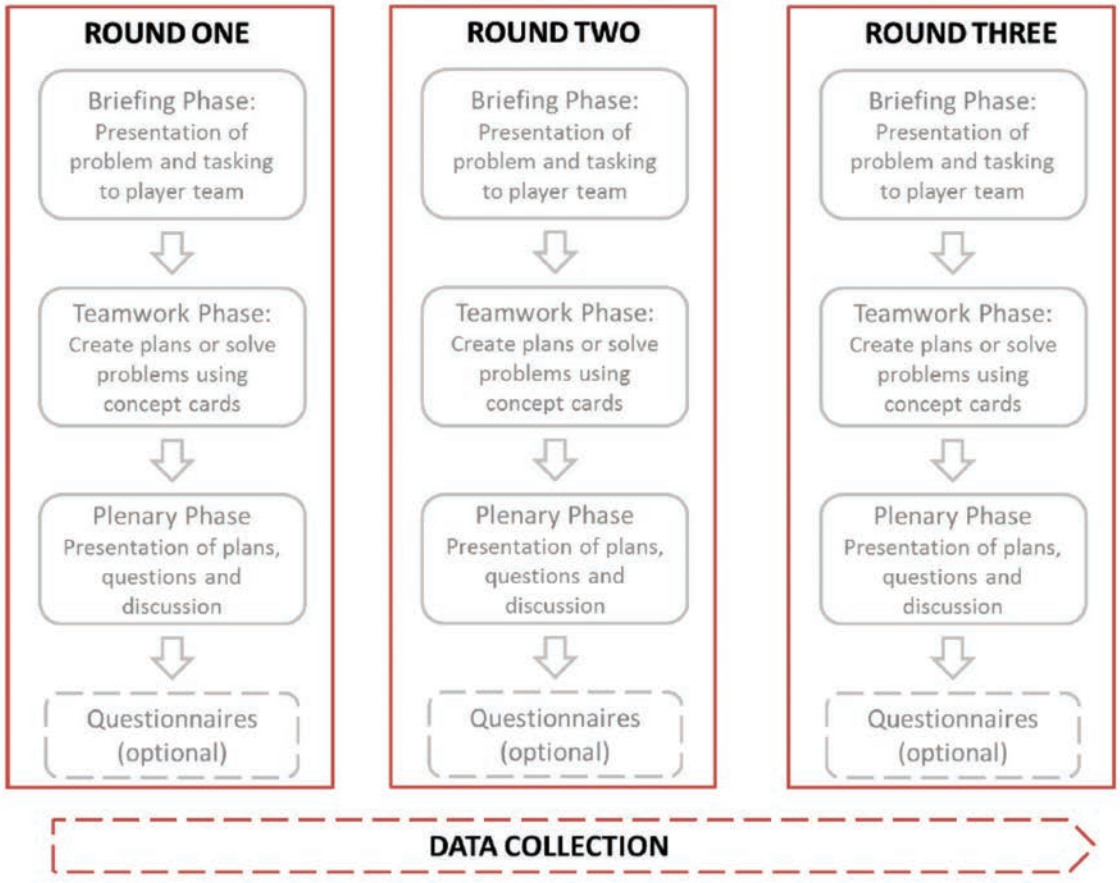


Figure 2 Phases and rounds in a CDAG
Source: NATO ACT 2014, 16.

Each round begins with an **introductory phase** conducted in plenary by all game teams, together with the moderator and the concept leader. During this phase, relevant aspects of the game are presented, such as the scenario, the specific vignette for the round, the problem to be solved, and the concept card that may be used to address the problem. This phase lasts approximately 10-15 minutes.

The scenario used can either remain consistent throughout all rounds or vary depending on the game's objectives and the concept being tested. However, to avoid confusing participants, it is recommended to use the same scenario throughout the entire CDAG. Additionally, employing a concise scenario design is a recognized CDAG practice (Collins and Hasberg 2018, 245) to prevent participants from becoming overwhelmed with details, ensuring their focus remains on the concept card being tested.

Each round involves a specific vignette, independent of others, situated within the scenario's context. The vignette provides teams with the necessary information to resolve the assigned problem, serving as the framework for discussions and analysis. Furthermore, the vignette outlines the role each game team assumes in addressing the given situation. It is important to note that all teams receive identical documents, roles, and tasks throughout the game.

During the introductory phase of each round, teams are also provided with a concept card specific to that round. This card contains either an excerpt or the entire concept intended for testing. The concept card serves as a potential tool for solving the problem outlined in the vignette. Teams can choose whether or not to use the card and are free to propose alternative solutions based on their preferences.

The second phase of the round, **the working phase**, focuses on identifying solutions to the given problem. It lasts approximately 90 minutes, with each team working separately in designated rooms. To generate solutions, teams may employ a variety of analysis methods and techniques that encourage critical thinking and explore alternative perspectives for addressing the problem, thereby enhancing the viability of the results (TRADOC G-2, Version 9.0 2022; UK Minstry of Defence 2021b; NATO ACT 2017). A simple and widely accepted technique that can be employed during the working phase is brainstorming, which stimulates creative thinking and the identification of innovative solutions (NATO ACT 2017, 31).

To ensure accountability and increase participant engagement, it is recommended that each round designate a team leader responsible for coordinating activities during the working session and presenting the conclusions during the plenary session. Additionally, as previously mentioned, each team should have at least one analyst assigned. The preparation of analysts is emphasized once again to ensure an efficient data collection process.

The next phase of each round, **the plenary phase**, is conducted jointly by all game teams under the guidance of the designated moderator and lasts approximately one hour. During this phase, the concept leader may also be present to ensure that the teams' responses are correctly understood and aligned with the theoretical framework of the study. Figure no. 3 illustrates the organizational structure of this phase for each round.

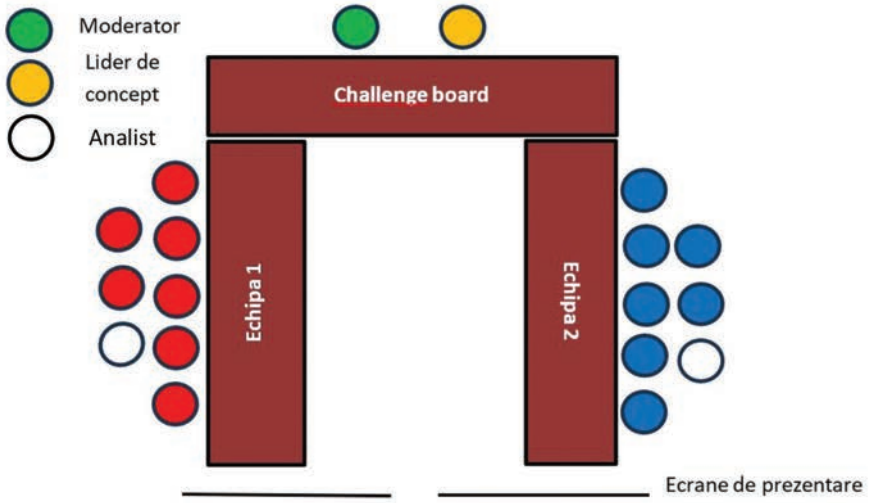


Figure 3 Plenary phase set-up
Source: NATO ACT 2014, 19.

During this phase, each team leader designated for the respective round presents the solutions their team identified to address the given situation. At the end of their presentation, members of the other team, the moderator, and the concept leader may ask clarifying questions about the presented information. This approach ensures a constructive discussion between the teams, with the potential to further develop and refine the solutions presented.

The final phase of each round may involve the completion of a **questionnaire** by all team participants to collect their direct feedback. This helps to better understand how they perceived the game's progression. The questionnaire aims to assess their level of understanding, the effectiveness, and the relevance of the concept card in solving the proposed challenges. It is worth noting that, for time efficiency, the methodology for completing these questionnaires is explained during the first day of the game, as part of the administrative activities, and should remain consistent across all rounds.

Arguments and considerations regarding the employment of CDAG in military research

There are numerous advantages to choosing the Concept Development and Assessment Game (CDAG) as a research tool. The mere fact that it is utilized by the world's largest alliance to develop its operational concepts is a compelling argument for adopting and integrating it into scientific research. Other **benefits of CDAG include**:

- Providing a framework for creative problem-solving in operational contexts, incorporating scientifically validated methods that facilitate critical thinking. This ensures the potential for innovative solutions that contribute effectively to the development of tested concepts (Feckler 2011, 2).

- Fostering open communication among team members, creating a space for the free expression of informed opinions.
- Economic testing of concepts, improving them at a low cost before they are tested in large-scale exercises (Collins and Hasberg 2018, 237).
- Reducing the risk of concept failure by enabling testing in a low-risk theoretical environment before practical application.
- Facilitating the identification and management of potential risks associated with the tested concept.
- Creating a forum for expert discussions, fostering opportunities to further develop the analysed concept.
- Offering flexibility, as the tool can be adjusted not only in relation to the concept being tested or the objectives set but also during the game's progression.
- Serving as a continuous learning method for participants. Scientifically proven methods for developing participants' critical and creative thinking skills can be integrated into the game (NATO ACT 2017, Foreward).
- Given the need for continuous adaptation of systems to the challenges of today's increasingly complex and volatile operational environment, CDAG can support the testing of new military concepts. The rapid technological evolution of contemporary society significantly influences the character of conflicts, and CDAG provides an economical, risk-free way to test new approaches, concepts, or operational methods for adapting armed forces to the current operational environment.

However, **the main advantage** of the Concept Development and Assessment Game (CDAG) is its ability to enable data collection through multiple methods, ensuring data triangulation. This feature is why we chose this title for our study. Three scientific data collection methods can be employed at different stages of CDAG: observation, focus groups, and questionnaires.
Data collection is carried out by analysts during team activities, plenary sessions for each round, and the final stage via administered questionnaires. Once the activity concludes, all analysts hand over their collected materials to the concept leader. Thus, CDAG provides a coherent framework for data collection.

During **the teamwork phase**, designated analysts collect data using **observation**, recognized as one of the main methods in qualitative research (Creswell 2013, 166); (Hennink, Hutter and Bailey 2020, 289; Saunders, Lewis and Thornhill 2019, 378). This method allows for a deeper understanding of the context, enabling the collection of rich and detailed data. In CDAG, analysts are advised to use an observation sheet provided by the concept leader on the first day of the game during administrative activities.
We reemphasize the importance of an analyst training session at the start of the activity to enhance data collection efficiency. Each observation sheet should also include methodological instructions to ensure the effectiveness of the data collection process.

Due to the structure of the game, the data collection method used during **the plenary phase** is the **focus group**. This method involves a moderated group discussion in which participants share their ideas on a specific topic (Crabtree and Miller 2023, 156). The organizational setup of CDAG, as previously described, aligns perfectly with the focus group method during the plenary phase. Additionally, the choice of focus groups is supported by the optimal group size for discussions, which academic literature suggests ranges from 4 to 15 participants (Krueger and Casey 2014, 33).

The qualitative nature of the game also aligns well with focus groups, as this method is almost always used to collect qualitative data (Stewart şi Shamdasani 2015, 42). Analysts collect data during this phase by electronically recording the entire discussion and noting the key debates on observation sheets also used during the teamwork phase. The advantage of this method is its interactive environment, which encourages innovative solutions through diverse perspectives based on each team's results.

The third data collection method applicable to CDAG is the **questionnaire**, recognized as suitable for qualitative research strategies (Charmaz 2014, 116). The questionnaire aims to understand the phenomenon and concept under study. It is essential to carefully design the questions to ensure methodological coherence with the game's qualitative approach. Open-ended questions are recommended, as they are well-suited to qualitative research practices, capturing participants' detailed perspectives related to the objectives.

The structure of the questionnaire must be logical, facilitating a coherent flow for respondents and potentially enhancing the quality of the responses. The guidance provided by Ian Brace and Kate Bolton in Questionnaire Design: How to Plan, Structure and Write Survey Material for Effective Market Research (Brace and Bolton 2022, 38-42) can serve as a valuable resource for planning data collection activities using this method.

To streamline the data collection process, electronic platforms like Google Forms can be employed. These systems often provide automatic charts and graphs of results, facilitating efficient data collection and analysis.
We must also acknowledge certain **limitations** of using such a structural framework for data collection. These represent weaknesses in the study that could potentially influence the results and conclusions of the research (Theofanidis and Fountouki 2018, 155).

First, the quality of the data is dependent on the analysts' experience in collecting it and their ability to capture elements truly relevant to the undertaken study. In this context, we reiterate the necessity of prior training to enhance their capacity to gather data aligned with the research objectives.
Additionally, while the game cannot replicate certain intrinsic psychological traits of armed conflicts, such as fear, fatigue, or stress (Popa 2019, 46), which military

personnel experience in real-life situations, it does provide a conducive environment for collecting qualitative data aimed at refining various military concepts.

It is also important to consider the methodological limitations inherent in the employed collection methods. Data obtained through observation is influenced by the observer's presence and subjectivity. Data from focus groups may be affected by conformity pressures on some participants and the influence of dominant opinion leaders. Meanwhile, data collected through questionnaires might be superficial, given that this method is applied at the final stage of the game.
All these limitations must be considered to ensure proper interpretation of the results and to transform the Concept Development and Assessment Game into an effective framework for data collection in scientific research specific to the military sciences domain.
Furthermore, **maintaining the methodological coherence** of scientific research is crucial. The Concept Development and Assessment Game is recommended exclusively for qualitative studies based on inductive reasoning, focusing on exploring military phenomena and identifying new solutions to current operational challenges.

It is advisable to select a qualitative research strategy consistent with the game's nature, which is to develop concepts in their early stages. For this reason, Grounded Theory (GT) may represent the most suitable research strategy. The essence of GT aligns with the organization of CDAG, as it is a qualitative approach involving systematic data collection and analysis, with constant refinement and comparison of results until a theory is developed (Charmaz and Thornberg 2021, 305). Thus, CDAG can support this process of refining theories and concepts.

Moreover, considering how the game is conducted, special attention must be paid to **ethical considerations**. All participants should be explicitly informed about the voluntary nature of their involvement in the study and their unconditional right to withdraw from the research without facing any negative repercussions. This ensures an appropriate environment for collecting valuable data, which is the primary premise for high-quality results.

Conclusions

The Concept Development and Assessment Game (CDAG) is a versatile tool that can make a substantial contribution to scientific research in the military field, providing an organized and efficient framework for testing operational concepts in their early stages of development. Through its adaptability, CDAG ensures the creative integration of data collection methods such as observation, focus groups, and questionnaires, fostering a qualitative scientific approach based on triangulation and result validation.

The main identified advantages, including its capacity to facilitate critical thinking, save resources, and manage risks within the testing environment, underscore the significant value of CDAG as a tool for developing military concepts. Furthermore, its flexibility and organizational structure allow for experimentation with new ideas and solutions, significantly reducing the risks associated with their direct implementation in the field. However, certain methodological limitations, particularly those related to the data collection methods used during the game, must also be analyzed and considered.

In conclusion, we regard CDAG as an extremely important tool for researching and developing military concepts, especially for young researchers. Despite its limitations, it offers a structured, ethical, and efficient approach to data collection, serving as a valuable resource for identifying viable solutions to ensure the continuous adaptation of military structures to the challenges of the contemporary operational environment.

References

Brace, Ian, and Kate Bolton. 2022. *Questionnaire Design: How to plan, structure and write survey material for effective market research.* 5th. London: Kogan Page Limited.

Braun, Virginia, and Victoria Clarke. 2013. *Successful qualitative research – a practical guide for beginners.* London: Sage Publications.

Charmaz, Kathy. 2014. *Constructing Grounded Theory.* 2nd edition. London: Sage Publications.

Charmaz, Kathy, and Robert Thornberg. 2021. "The pursuit of quality in grounded theory." *Qualitative research in psychology* 18 (3).

Collins, Sue, and Marcel-Paul Hasberg. 2018. "Tabletop Assessment Games in Concept Development and Experimentation„" In *Advances in Defence Analysis, Concept Development and Experimentation: Innovation for the Future*. Norfolk: NATO HQ Supreme Allied Command Transformation.

Crabtree, Benjamin F., and William L. Miller. 2023. *Doing Qualitative Research,* 3rd. Los Angeles: Sage Publications.

Creswell, John C. 2013. *Qualitative inquiry and research design: choosing among five approaches.* Londra: Sage Publications.

Dawson, Catherine. 2019. *Introduction to research methods: A practical guide for anyone undertaking a research project, ed. 5.* Robinson.

Feckler, D. 2011. „ACT Employs Analytical War-Game." *The Transformer, Bi-Annual Publication of Allied Command Transformation*, 2.

Hennink, Monique, Inge Hutter, and Ajay Bailey. 2020. *Qualitative Research Methods.* London: Sage Publications.

—. 2020. *Qualitative Research Methods.* London: Sage Publications.

Joint Doctrine Note 1-19. 2019. *Competition Continuum.* US Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jdn1_19.pdf.

Krueger, Richard A., and Mary Anne Casey. 2014. *Focus Groups: A Practical Guide for Applied Research.* 5th. Los Angeles: Sage Publications.

Leavy, Patricia. 2023. *Research Design - Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches, Second edition.* New York: The Guilford Press.

—. 2020. *The Oxford Handbook of Qualitative Research.* 2nd. Oxford: Oxford University Press.

Mazarr, Michael J., Jonathan S. Blake, Abigail Casey, Tim McDonald, Stephanie Pezard, and Michael Spirtas. 2018. *Understanding the Emerging Era of International Competition. Theoretical and Historical Perspectives.* Santa Monica, California: RAND Corporation.

Mazarr, Michael J., Jonah Blank, Samuel Charap, Benjamin N. Harris, Timothy R. Heath, Niklas Helwig, Jeffrey W. Hornung, Lyle J. Morris, Ashley L. Rhoades, Ariane M. Tabatabai, Sean M. Zeigler. 2022. *Understanding the Emerging Era of International Competition Through the Eyes of Others. Country Perspectives.* Santa Monica, California: RAND Corporation.

MCDP 1-4. 2020. *Competing.* U.S. Marine Corps. https://www.marines.mil/News/Publications/MCPEL/Electronic-Library-Display/Article/2449338/mcdp-1-4/.

Moser, Albine, and Irene Korstjens. 2018. "Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis." *European Journal of General Practice* 24 (1).

NATO ACT. 2021. *NATO Concept Development and Experimentation Handbook: A concept developer's toolbox.* Norfolk: NATO Allied Command Transformation.

—. 2014. *NATO Concept Development Assessment Game "CDAG" Handbook.* Norfolk: NATO Allied Command Transformation.

—. 2017. *The NATO Alternative Analysis Handbook, second edition.* Norfolk: NATO Allied Command Transformation.

—. 2011. *Transformer.* Norfolk: NATO Allied Command Transformation.

Nistorescu, Claudiu Valer. 2024. "Adaptarea organizației militare – O condiție esențială pentru obținerea succesului pe câmpul de luptă." *Gândirea Militară Românească* (3): 194-209.

Popa, Marian. 2019. *Psihologie militară.* Editia a doua. București: Editura Polirom.

Rassel, Gary, Suzanne Leland, Zachary Mohr, and Elizabeth Ann O'Sullivan. 2020. *Research methods for public administrators.* Routledge.

Ravitch, Sharon M., and Nicole Mittenfelner Carl. 2021. *Qualitative Research. Bridging the Conceptual, Theoretical, and Methodological.* 2nd. London: Sage Publications.

Salmons, Janet E. 2022. *Doing Qualitative Research Online.* London: Sage Publications.

Saunders, Mark N.K., Philip Lewis, and Adrian Thornhill. 2019. *Research Methods for Business Students.* 8th edition. Pearson Education.

Sharan B. Merriam, Robin S. Grenier. 2019. *Qualitative Research in Practice. Examples for Discussion and Analysis.* 2nd. San-Francisco: Jossey-Bass.

Stewart, David W., and Prem N. Shamdasani. 2015. *Focus Groups: Theory and Practice.* 3rd edition. Los Angeles: Sage Publications.

Theofanidis, Dimitrios, and Antigoni Fountouki. 2018. "Limitations and delimitations in the research process." *Perioperative Nursing-Quarterly scientific, Online Official Journal of GORNA* 7 (3).

TRADOC G-2, Version 9.0. 2022. *The Red Team Handbook. The Army's guide to making better decisions.* 9. US Army Training and Doctrine.

UK Ministry of Defence. 2021a. *Defence Experimentation for Force Development Handbook.* https://assets.publishing.service.gov.uk/media/6014030be90e07626914df3c/20210121-DEFD_Handbook_Version_2-O.pdf.

__. 2021b. *Red Teaming Handbook.* 3rd. https://assets.publishing.service.gov.uk/media/61702155e90e07197867eb93/20210625-Red_Teaming_Handbook.pdf.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

The foundation for a joint fire support capability using the NATO model

LTC Adrian MIREA, Ph.D. Candidate*
*"Carol I" National Defence University, Bucharest, Romania
e-mail: mirea.adrian82@gmail.com

Abstract

Providing joint fire support is an indispensable capability for joint forces that facilitates the achievement of set objectives in all types of operations. Starting from the idea that the development of a fire support doctrine, currently non-existent at the national level, is not sufficient to achieve this capability at the joint force level, I have argued in this paper, other changes that I consider necessary using the NATO capability development model, described by the acronym DOTMLPF-I. In the first part of the article, I have briefly presented the components of the NATO model and then, in the second part, I address the fire support capability as a whole, in terms of doctrine, force structure organization, training, the need to review the available resources, the training of military leaders and fire support personnel, the existing infrastructure and the level of interoperability required to make this capability truly available to the armed forces structures. The actions identified in the eight strands of the NATO model can provide a perspective for developing or enhancing the capability to provide nationally-led joint fire support.

Keywords:
fire support; joint fire support; capability; NATO model; DOTMLPF-I.

Article info
Received: 25 October 2024; Revised: 21 November 2024; Accepted: 3 December 2024; Available online: 17 January 2025

Citation: Mirea, A. 2024. "The foundation for a joint fire support capability using the NATO model". *Bulletin of "Carol I" National Defence University*, 13(4): 184-193. https://doi.org/10.53477/2284-9378-24-57

Currently, at the national level, there is no common doctrinal framework that implements in a unified manner the way to provide fire support at the joint level; the force structures belonging to joint force components each have their own doctrines and field manuals detailing fire support. In addition to the need to have a joint fire support doctrine developed and implemented through all categories of national armed forces, I considered it useful to identify ways to base this capability to provide joint fire support (through an exclusively national effort) on the NATO model of capability development, known by the acronym DOTMLPF-I (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability (NATO 2021, 7). As an argument for choosing this model, I mention that Romania's Military Strategy of 2016, in Chapter IV Defense Capabilities and Priorities for their realization, bases actions on the eight directions described by the NATO model in order to achieve credible and sustainable defence capabilities (Portal legislativ 2016).

The analysis of an existing or determined capability as necessary to meet a new requirement, using the NATO model specified above, may argue the need for changes, material or non-material, in the form of actions in any of the eight directions described by the acronym DOTMLPF-I. Having argued the need for the development of a joint fire support doctrine in a recently published article "*Implementing a Joint Fire Support Doctrine – A Joint Operation Requirement*", (Mirea and Stanciu 2024) dealing basically only with the first direction under the DOTMLPF-I acronym, I found it useful to address the joint fire support capability as a whole, in all aspects described by the NATO model.

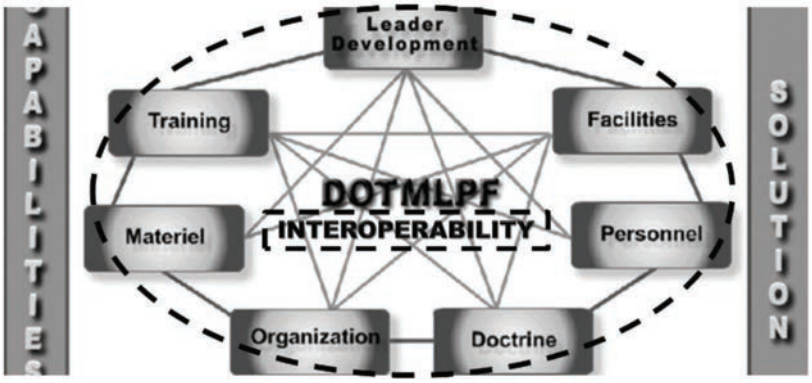


Figure 1 NATO model for capability development
Source: Adaptation from MD Harris Institute 2013.

As the development of a joint fire support doctrine may not be sufficient to build a joint fire support capability, I have set out in this paper to briefly identify and argue potential actions in all eight of the above-mentioned directions to build or develop a national joint fire support capability.

In developing this article, I have explored mainly open sources of information in the form of websites and authored works to which I have added unclassified doctrines

and field manuals in force at the national and NATO level, which detail relevant aspects of providing fire support at the joint level and argue potential actions to substantiate a capability according to the NATO model. The collection, analysis and interpretation of the data from the sources explored were systematically carried out based on documentary analysis (Okoko, Tunison and Walker 2023, 140), a method that ensured my understanding and synthesis of the main aspects of the subject of this paper.

DOTMLPF-I utility in the foundation of a capability

The Analysis Framework, described by the acronym DOTMLPF-I, is a tool or methodology (Willi 2016) useful, in my view, both for substantiating a new capability and for identifying shortfalls or deficiencies in the approach to an existing capability - the provision of joint fire support in this case. The usefulness of this analytical tool lies in systematically addressing all (interrelated) aspects that may influence the availability of a capability. Changes to a single element - such as the development of a doctrine for joint fire support - will not have the desired operational effect because, depending on the entity under analysis, other changes may be identified as necessary, such as changes in the organizational level or in the interoperability of joint force components, in order for the desired capability to be actually achieved or enhanced. The purpose of using such an analytical tool in the case of a joint fire support capability is to increase the level of joint force effectiveness in exploiting the potential of fire support systems available at its component level.

The ***doctrinal*** course of action aims to implement or update the fundamental principles for the employment of force structures, which are usually contained in existing national doctrines. In our case, we do not have a national joint fire support doctrine, but if one existed, the NATO model analysis would have aimed at its possible refinement, so that the content elements or specific terminology in the field of providing joint fire support would reflect an updated approach to the capability pursued.

Actions in the field of the ***organization*** pay attention to the structural functionality of the forces in order to identify possible shortcomings or needs for updating the way individuals or components of force structures cooperate systematically to achieve the entrusted objectives. The focus of the analysis in this direction is on how to leverage the targeted capability within the existing organizational context. Some needs for organizational adjustment can thus be identified so that the targeted capability is revealed to its full potential.

Concerning ***training***, actions in this direction concern the way in which individuals, sub-units, units and staff are prepared or trained to implement doctrinal provisions, field manuals or existing tactics, techniques and procedures in order to accomplish the mission. From the perspective of a new or developing capability (in the process

of acquisition, equipping, deployment, etc.) at the force structure level, training is central to understanding the full range of operational implications that the availability of this emerging capability has.
The action line on ***materiel*** aims at the equipment component of a capability. Analysis in this area may identify possible needs to modify existing quantities of military equipment or highlight the need for new acquisitions so that the capability is truly operational in all respects.

Leadership actions aim at the professional preparation of military leaders - a product of continuing education - incorporating training, expertise, education and personal development. Moreover, leadership is the foundation of command - the art of motivating and directing personnel. Changes in this direction are required when there are some shortcomings in the utilization of the targeted capability due to the level of professional competence of individuals.
The analysis and identification of measures in the area of ***personnel*** are based on the existence of qualified personnel to capitalize on the capability under study. The categories of personnel that comprise the force structures and their basic skills can have a significant impact on how to exploit the full potential provided by an available capability.

From the ***facilities*** domain perspective, the potential actions focus on the infrastructure elements necessary for the effective exploitation of the targeted capability. In this category of actions, the buildings, structures, related utilities, land and fire ranges required for operating the capability under analysis are targeted.

The potential changes in ***interoperability*** direction pursue actions in its three characteristic areas of interoperability - technical, human and procedural. As a NATO-level capability development model, interoperability is essential, as allied force structures must perform in a multinational operating environment. Moreover, from a NATO perspective, interoperability is even seen as a force multiplier (NATO 2023).

NATO model (DOTMLPF-I) applicability in funding a capability

As mentioned above, the analysis framework described by the acronym DOTMLPF-I, is a useful tool, both for substantiating a new capability and for identifying shortfalls or deficiencies in the approach to an existing capability. The capability analyzed through these eight domains' perspectives is the provision of joint fire support.

Starting from the idea that, at present, there are some shortfalls in providing joint fire support - such as the lack of a doctrinal framework - I have set out to present a perspective on the foundation of this capability with national armed forces using the NATO model in the way I have observed it being used at the alliance level (NATO 2018).

Doctrine

The joint fire support doctrine is the basic regulation underpinning the common conceptual framework and specific terminology required by commanders and staff in planning and providing joint fire support according to the concept of operation (NATO 2015, VII). The lack of such a doctrinal regulatory framework at the national level, to implement in a unified way the fundamental concepts of joint fire support in all categories of armed forces, led me to argue the need to eliminate this shortcoming in the aforementioned article "*Implementing a Joint Fire Support Doctrine – A Joint Operation Requirement*" (Mirea and Stanciu 2024).

The first and most important doctrinal action to substantiate the capability to provide joint fire support is the development of such a regulation at the highest hierarchical level of national military authority. It is the joint fire support doctrine that describes the fundamentals of the capability under study, but it is also a guide to best practices for the joint force commander and his staff in the use of the fire support systems provided by the component force categories. The development of the doctrine will ensure the coherent implementation of key concepts such as standard tactical missions or fire support coordination measures, so that the full potential of the joint fire support capability can be achieved effectively and safely for friendly forces.

Organization

The need for action in this direction is directly dependent on the implementation of ongoing or prospective procurement programs for military equipment components of the fire support system. For example, the equipping of ground force structures with M142 HIMARS (High Mobility Artillery Rocket System) (Mureşan 2024) implies some organizational changes at the unit level in order to be able to operate such systems, and it is probably necessary to review the functions of the crew within groups/pieces/installations since HIMARS systems require a small number of operators compared to the artillery systems they replace. It should be noted that such reorganizations within military units are reflected in classified documents not the subject of this paper.

The need for organizational changes is all the more evident in view of national ownership of capability requirements within NATO. The transformations implied by the disappearance or replacement of old fire support systems, in conjunction with the gradual implementation of acquisition programs, come with new challenges also from an organizational point of view. These, in turn, need to be reflected in the updating of existing field manuals that regulate and detail how individuals, sub-units and units systematically cooperate for operational efficiency. A temporary solution to ensure the exploitation of the full potential of the joint fire support capability, regardless of the current organizational situation of the national armed forces, may be, in my view, the implementation and permanent updating of Standard Operating Procedures (SOPs) at every command level in order to ensure standardization and preserve the efficiency of force structures (James 2020).

Training

In the absence of a joint fire support doctrine, as mentioned above, national armed force categories are guided by their own doctrines and field manuals governing the way how to provide fire support. Joint training of the responsible actors within the components of the joint force can develop and strengthen the joint fire support capability. The objectives of military exercises include the joint training of participants, especially those from different branches of the joint force, to enhance interoperability at the joint and alliance levels (SMFT 2019). Exercise scenarios provide the framework for joint training of command staff to plan and conduct actions according to a single concept of operations.

In this context, one line of action to strengthen the capability to provide joint fire support is to identify and counter the shortfalls caused by differences of perspective between force categories on basic concepts in the field of fire support. These shortcomings are, in my view, an effect of the aforementioned lack of a common doctrinal framework, as each category of armed forces has its own regulations in this area. At the moment, concepts such as *standard tactical missions* or *fire support coordination measures* are not similarly understood and implemented across all categories of national armed forces. For example, the standard tactical mission *direct support*, which can be assigned to a fire support structure, is detailed differently in land forces than in naval forces. Land force structures implement the provisions of NATO fire support doctrine AArtyP-5(B), NATO Fire Support Doctrine (NATO 2015, 3-2) and naval force structures implement the provisions of Allied Joint Maritime Operations doctrine AJP 3.1, Allied Joint Maritime Operations.

The training of those responsible for providing fire support from land force structures together with liaison officers from other categories of armed forces - components of the joint force, ensures the identification of shortfalls in the exploitation of joint fire support capabilities and can lead to the implementation of solutions to overcome them, such as SOPs.

Materiel

The national equipping programs, recently carried out or currently under implementation (MApN 2024) may generate some challenges in capitalizing on new capabilities available to the force structures alongside the existing ones. Thus, equipping with modern equipment and the replacement of obsolete ones determines not only a revision of the field manuals in force but also a review of the amount of military equipment available in order to ensure the efficiency of the structure in relation to its core mission.

Another action in this direction to strengthen the joint fire support capability is to understand that changes in the field of force structure equipping have an impact on the whole structure of the operations conducted. For example, equipping land force structures with HIMARS systems has an impact on each component of the

structure of operations (combat, striking or engineering systems) and implies a review of resource quantities by forces so that these new fire support capabilities can be truly exploited in the operation. If we consider issues such as the need for adequate ammunition supply or the additional need for air and missile (anti-drone) protection of HIMARS systems, we can conclude that equipping with such modern systems requires a review of the amount of military equipment of all types available to the force.

Leadership

Given that leadership is, as mentioned above, a product of continuing education that builds on the training, expertise and personal development of individuals, enhancing the capability to provide joint fire support can be achieved through actions in all these areas. The ultimate aim is to develop and maintain the optimum level of professional competence, primarily for those responsible for providing fire support at the level of force structure commands.

An important point from my point of view is that, in accordance with the national regulations in force, those responsible for providing fire support at the joint level come from the ranks of field artillery officers (SMFT 2018, I-2). Accordingly, actions to strengthen the capability to provide joint fire support must be focused on optimized training of these officers throughout their careers, developing their joint fire support conceptualization skills across all the functions they occupy and all the career courses they attend.

A concrete action to achieve the proposed goal could be, in my view, to adjust the curricular structure of the programs of all career courses in order to integrate fire support systems from other categories of national armed forces into the training of these officers.

Another concrete action could be to integrate fire support systems from other categories of national armed forces into all exercises conducted by those responsible for providing fire support in land forces. For example, the brigade-level fire support coordinator, who is also the commander of the organic field artillery battalion, will also have at his disposal some air force or naval fire support systems during exercises to integrate them into the fire support plan of his land structure.

Actions in this direction of leadership aimed at an adequate professional training of individual military leaders are a feature of the study programs of the Command and Staff Faculty of the "Carol I" National Defense University as they have established through the graduate model the qualities necessary for military leaders at all levels of command. The joint-level exercises conducted at the National Defense University have among their objectives the development of essential skills for trainee and student officers in leading military actions. Land forces fire support officers benefit from the expertise of air and naval colleagues, established as liaison officers at the command level, to plan and provide joint-level fire support during exercises.

Personnel

Actions in this area are closely linked to those in the area of leadership but are aimed at ensuring that all categories of personnel involved in exploiting the joint fire support system in operation have the necessary skills. The essential personnel, in my view, for the provision of joint-level fire support are those who staff (or augment in the case of liaison officers) the force structure commands. They are the main specialists but also the responsible officers who must have the necessary skills to operate the joint fire support system in an operation. Thus, the appropriate professional training of all personnel (regardless of force category, weapon or basic speciality) participating in fire support cells/working groups is very important in order to realize the full potential of the joint fire support capability.

Facilities

The existing facilities at the national level provide, in my view, the minimum necessary conditions for the exploitation of the joint fire support capability, as the national armed forces have at their disposal a multitude of infrastructure elements for the training, exercising and employment of fire support systems. The specific needs for modernizing or improving current conditions offered by the available facilities are constantly analyzed at the level of each category of forces.

An action in this direction could be, in my view, to analyze the opportunity of having a national firing range that would allow the long-range use of very long-range fire support systems, such as HIMARS systems that have ammunition with a range of up to 300 km or Bayraktar drones. With the introduction of new or upgraded fire support systems into the national armed forces structures, such needs may also arise. Existing national firing ranges provide for the use of these munitions, but within certain limits, the ranges having been developed and approved for capabilities that existed at a certain point in the past.

Interoperability

Actions in this area aim to ensure technical, human and procedural interoperability so that the personnel and equipment that make up the fire support systems at the level of the categories of national armed forces can really underpin the capability to provide fire support at the joint level.

The development of joint fire support doctrine and the use of standard operating procedures, as mentioned above, addresses the need for the procedural interoperability required for joint fire support capability.

The joint training of fire support officers from all categories of national armed forces in joint-level military exercises covers the human interoperability requirement for the joint fire support capability.

Technical interoperability is the most problematic, in my view, because achieving it requires the acquisition of specialized systems such as automated command and control systems or automated fire control systems. The full potential of fire support

systems available to a joint force depends on such systems. An example is the International Field Artillery Tactical Data System (IFATDS), available to HIMARS-equipped structures, which in my view needs to be integrated with equally modern command and control or ISR (Intelligence, Surveillance and Reconnaissance) systems so that the full potential of HIMARS systems can be exploited.

Conclusions

The implementation of current or prospective equipping programs, which involve the acquisition and introduction of various modern military equipment into the national armed forces structures, also brings certain challenges in terms of exploitation and optimized use of the capabilities thus acquired. In addition to the direct, easily perceptible advantages that the new military equipment brings to force structures, all the implications that they have for exploiting them to their full potential in an operation must also be taken into account. Thus, the organizational changes imposed by new equipment, as reflected in the organizational structure, must be accompanied by reviews of related areas directly or indirectly linked to their exploitation, such as the training of personnel responsible for using the equipment, the existing facilities for training individuals, teams, squads or units, the quantities of resources allocated to the beneficiary structures, the degree of interoperability of the equipment and so on.

The analysis model, deployed along the eight courses of action of the acronym DOTMLPF-I, is a useful tool to understand all the implications of the timely exploitation of a new capability and also to outline a perspective for optimizing an existing capability. In this paper, I have used this tool to systematically address each aspect under which the capability under study - the provision of joint fire support - can be enhanced through concrete actions in the eight directions. I have thus identified some shortcomings in the current exploitation of the national fire support system and, at the same time, I based actions in the form of proposals to improve the capability to provide joint fire support at the national level.

The capabilities assumed by our country as a contribution to NATO's collective defence planning, analyzed also on the DOTMLPF-I model, are those that constitute the basis for acquisition needs or the need to change certain aspects on the eight directions so that these assumed capabilities are really developed and strengthened at the national level.

References

James, Randy. 2020. "Standard Operating Procedures: This is the way we've always done it." *U.S. Army.* https://www.army.mil/article/238732/standard_operating_procedures_this_is_the_way_weve_always_done_it.

Ministerul Apărării Naționale [MApN]. 2024. *Programe de înzestrare.* https://www.dpa.ro/programe-de-inzestrare/.

MD Harris Institute. 2013. *DOTMLPF-P Analysis for War and Peace.* https://mdharrismd.com/2013/11/09/dotmlpf-p-analysis-and-military-medicine/.

Mirea, Adrian, and Cristian-Octavian Stanciu. 2024. "Implementarea unei doctrine a sprijinului prin foc de nivel întrunit – cerință a operației întrunite." *Colocviu Strategic* (Nr. 1): 1-6.

Mureșan, Darius. 2024. "Câte HIMARS are România și când ajung ultimele sisteme în țară. Armata deține inclusiv celebrele rachete ATACMS ce lovesc la 300 km distanță." *Defense Romania.* https://www.defenseromania.ro/cate-himars-are-romania-si-cand-ajung-ultimele-sisteme-in-tara-armata-detine-inclusiv-celebrele-rachete-atacms-ce-lovesc-la-300-km-distanta_629999.html.

NATO. 2015. *NATO FIRE SUPPORT DOCTRINE AArtyP-5.* NATO: NATO Standardization Office.

—. 2018. *NATO's Joint Air Power Strategy.* https://www.nato.int/cps/en/natohq/official_texts_156374.htm?selectedLocale=en.

—. 2021. *NATO CD-E Handbook, A concept developer`s toolbox.* Norfolk: Allied Command Transformation.

—. 2023. *Interoperability: connecting forces.* https://www.nato.int/cps/en/natohq/topics_84112.htm.

Okoko, Janet Mola, Scott Tunison, and Keith D. Walker. 2023. *Varieties of Qualitative Research Methods.* Saskatoon, Saskatoon: Springer Texts in Education.

Portal legislativ. 2016. „Strategia militară a României din 28 septembrie 2016." Publicat în Monitorul Oficial, nr. 789, din 7 octombrie 2016. https://legislatie.just.ro/Public/DetaliiDocument/182367.

Statul Major al Apărării [SMFT]. 2018. *Manualul sprijinului prin foc în operațiile grupării de forțe F.T.-6.* București: MApN.

—. 2019. „Noutăți SG19". https://www.defense.ro/sg19/noutati.

Willi, Bernie. 2016. "Assessing Nations for NATO Partnerships." *Transforming Joint Air Power. The journal of the JAPCC* 51-54.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Personality profile of high-performing leaders: a BFI-2 analysis

LTC Cristian PANAIT, Ph.D.*
* "Henri Coandă" Air Force Academy, Brașov
e-mail: cristian.panait@afahc.ro

Abstract

The present study employs a Big Five Inventory-2 (BFI-2) analysis to investigate the personality traits of a group of high-performing leaders operating within a military context. The Big Five Inventory-2 (BFI-2), T-score analysis, and Variance analysis (ANOVA) were utilized to identify the personality configurations contributing to effective leadership in military environments. The findings indicate that "Emotional Stability" and "Conscientiousness" are the most salient traits, with high scores for "Productivity," "Responsibility," and low "Emotional Volatility." These traits, essential for goal-oriented behaviour and resilience under stressful conditions, are in accordance with previous research, linking these traits to job performance and stress management in leadership roles. A moderate level of Extraversion and Agreeableness is beneficial for maintaining normal team dynamics and fostering trust. Similarly, a balanced level of Openness to Experiences is associated with strategic adaptability without compromising discipline and performance. The study validates the utility of the BFI-2 in identifying personality traits that are predictive of success in exercising leadership in high-stress environments; it also highlights the distinction between leaders and the mean of the general population on these traits. The results indicate that the enhancement of these traits may result in increased leadership effectiveness, thus providing insights for the improvement of human resources selection and training programs.

Keywords:
High-Performing Military Leaders; Big Five Inventory-2 (BFI-2); Personality Traits; Conscientiousness; Emotional Stability; Leadership; Personality Assessment; Human Resources Selection and Training.

Article info
Received: 14 November 2024; Revised: 29 November 2024; Accepted: 10 December 2024; Available online: 17 January 2025

Citation: Panait, C. 2024. "Personality profile of high-performing leaders: a BFI-2 analysis". *Bulletin of "Carol I" National Defence University*, 13(4): 194-205. https://doi.org/10.53477/2284-9378-24-58

This paper presents the personality profiles of a group of high-performing leaders in a military context, using the Big Five Inventory - 2 (BFI-2) to identify predominant personality traits and *T-scores* to relate the results to the general population. The study was conducted for the dissertation paper prepared at the end of the Master of Joint Command - Air Forces at the Command and Staff Faculty of "Carol I" National Defence University - Bucharest. The study for the dissertation contains more complex research due to the fact that personality traits were identified to validate a hypothesis of predictability of association with certain leadership styles based on predominant personality traits.

In this study, the term "high-performing leaders" refers to individuals in leadership positions who consistently demonstrate superior performance in achieving organizational goals, managing responsibilities, and maintaining resilience under pressure. These characteristics are essential and define the work of a military officer who is successful in career advancement in responsibility-sensitive leadership positions. The sample is comprised of military officers who have been admitted to a military graduate school after a rigorous selection process, officers who have demonstrated not only intent, dedication, and sacrifice by committing personal time to complete rigorous training, but also the competence to perform leadership roles in specialized military fields. The officers' branches range from fighter pilots, pilots, and air traffic controllers to air defence officers. These criteria to differentiate high-performing leaders are in line with studies such as S. Singh (2003) that higher-performing leaders foster team adaptability and cohesion in high-performance contexts, DM Hutton (2018) on situational adaptability and interpersonal effectiveness in high-risk environments, and P. Hawkins (2014), who emphasizes that higher-performing leaders excel at building effective teams and accomplishing goals.

Understanding personality traits that contribute to effective leadership is a focus of interest in psychological research, with the Big Five personality model emerging as a relevant (Cronbach Alpha = 0,86), scientifically accepted framework. The Big Five Inventory - 2 (BFI-2) is an evolution of the original Big Five Inventory, providing a tool for measuring personality traits associated with leadership potential and performance. Developed by Soto and John (2017), the BFI-2 expands the scope of personality assessment by introducing a hierarchical model that includes 15 facet-level factors or traits within the five major meta-factors *Extraversion, Agreeableness, Conscientiousness, Emotional Instability* (Negative Emotionality or Neuroticism), and *Open-Mindedness to Experiences* (Open-Mindedness). By performing both general and detailed analysis, the BFI-2 offers increased predictive power and reliability and is relevant for assessing traits that support leadership.

Personality assessment using the Big Five model has consistently proven its relevance in organizational settings where certain personality traits are correlated with leadership effectiveness. Research indicates that high levels of *conscientiousness* and

emotional stability are particularly associated with leadership effectiveness, as these traits foster goal-oriented behaviour, resilience and stable decision-making. High *Conscientiousness*, characterized by traits such as *Productivity*, *Organization*, and *Responsibility*, enables leaders to adopt a disciplined approach, essential for dealing with complex demands. *Emotional Stability*, represented by low scores on the *Anxiety* and *Emotional Volatility* factors, enables leaders to effectively manage stress, an important factor in situations that require quick thinking and calm decision-making.

BFI-2's ability to assess traits using *T-scores* facilitates a standardized measure of trait intensity across diverse populations. *T-scores* adjust individual scores relative to a normative sample, allowing comparative analysis of how certain traits may vary among leaders relative to the general population. In the field of leadership studies, *T-scores* provide valuable insight into how the intensities of factors such as *Conscientiousness* and *Emotional Stability* can predict a leader's success in diverse contexts, particularly in high-risk environments such as the military, where resilience and discipline are essential.

Previous research emphasizes the importance of certain Big Five model traits in improving leadership performance; Judge et al. (2002) found that, although *Extraversion* may be less prevalent than *Conscientiousness* and *Emotional Stability*, it still contributes to leadership by promoting positive social interactions, assertiveness and effective team communication. *Agreeableness*, although not very often associated with leadership because of the potential to reduce authoritative firmness of command, can nonetheless improve trust and group harmony, especially in leaders who score high on facets such as *Trust* and *Respect*. Therefore, moderate levels of *Agreeableness* can create a balanced approach that encourages teamwork without compromising authority.

Through the *T-score* analysis, the research provides a comparative perspective on the intensity of the traits, revealing significant increases in *Conscientiousness* and *Emotional Stability* across the sample. These findings contribute to the understanding of how certain factors in the Big Five domains align with effective leadership, providing detailed insight into the role of personality in predicting leadership success. This research is also relevant because organizations are increasingly relying on personality assessments, such as the BFI-2, for selection and training in a variety of areas.

Research methodology and objectives

This study employs a quantitative and comparative methodology to examine the personality traits of high-performing military leaders using the Big Five Inventory-2 (BFI-2). The raw scores were transformed into T-scores, allowing standardized comparison with a normative population and facilitating an understanding of

personality traits predictive of leadership success.
The study's focus on military leadership in high-stress environments guided the formulation of the following research questions:

1. What are the most pronounced personality traits among high-performing military leaders as identified by the BFI-2?
2. How do these traits compare to those of the general population using normative T-scores?

By addressing these research questions, this study aims to identify the key personality configurations associated with effective leadership.

The BFI-2 was chosen as the research instrument because of its demonstrated validity in measuring both personality traits across multiple cultures and general populations as well as specific personality traits, such as the military. This research instrument contains 60 items grouped into five Meta-Factors: *Extraversion, Agreeableness, Conscientiousness, Emotional Instability, and Openness to Experiences*, along with 15 factors that allow for more detailed analysis within each Meta–factor. The selection of BFI-2 is consistent with research emphasizing the importance of face-level perspectives for the predictability of certain leadership outcomes (Soto and John 2017). For example:

- *Conscientiousness*: Factors such as productivity, accountability, and organization are particularly relevant because of their association with goal (mission) oriented behaviours, reliability, and attention to detail. Leaders who score high on these factors are more likely to excel in roles that require discipline and consistency.
- *Emotional instability*: Low scores on factors such as *anxiety*, *emotional volatility* and *depression* indicate emotional stability, an important trait for leaders operating in stressful environments. This stability allows leaders to remain calm and focused for rational decision-making in dynamic or crisis situations.
- *Extraversion* and *Agreeableness*: Moderate scores on factors such as *sociability*, *assertiveness* and *trust* were assessed to understand their role in enhancing team dynamics and developing interpersonal relationships. In leadership, these traits create a balance between authority and approachability, contributing to team cohesion and team morale.
- *Openness to experiences*: *Creative imagination* and *intellectual curiosity* were rated as indicators of adaptability and openness to new ideas, traits that are beneficial for leaders who have to work in complex and constantly changing environments.

Presentation of the focus group

The study sample consisted of 29 individuals, out of a total of 30 officers from the Romanian Air Force who were attending the Master's Degree program in Joint

Command, Air Force specialization. In order to maintain objectivity, I excluded myself from the sample.

These officers were admitted after a rigorous selection process, demonstrating the dedication and competence required for leadership positions; all officers had senior officer ranks with a minimum of 15 years of experience in the act of military leadership. Their specializations include fighter pilots, air traffic controllers, and air defence officers, reflecting a diverse range of military fields where adaptability, discipline, and decision-making ability are essential. This context ensures that the sample accurately represents a high-performance and leadership-oriented group suitable for examining personality traits associated with effective leadership. From a psychological point of view, this group is a homogeneous one because the career selection was done including the admission to psychological examinations that are periodically administered. To investigate the potential interactions between the key personality traits associated with effective leadership, the variables *Conscientiousness* and *Emotional Stability*, a dispersion analysis (ANOVA) was conducted, given that there were two groups in the sample, first and second-year officers. This approach allowed us to test for significant interaction effects between these traits across different levels of training, providing a more detailed understanding of how these combined traits may influence leadership performance. By examining the interplay between *Conscientiousness* and *Emotional Stability*, the analysis aimed to uncover differences in the combined effects of these traits between the two groups, thus contributing to the assessment of leadership potential at different stages of officer training. However, the presentation of these results may be the subject of another article.

Creating a study group of only military officers limits the possibility of generalizing the findings to other occupational contexts; future research could extend these findings to other professions that involve functioning in stressful situations, such as healthcare, law enforcement, or even corporate, to determine whether similar personality profiles produce leadership effectiveness. In addition, examining longitudinal changes in personality traits among leaders could provide insights into how traits such as *conscientiousness* and *emotional stability* develop or fluctuate over a leader's career, or whether they are stable, or fixed.
Personality is considered to be relatively fixed with age, with insignificant changes occurring after age 30. In a study (Srivastava et al. 2003, 1041 - 1053) conducted on a sample n = 132,515 individuals it was found that *agreeableness* and *conscientiousness* increased during early and middle adulthood and emotional stability decreased among women but not men.

Evaluation procedure

The BFI-2 was administered in a controlled, face-to-face environment to ensure consistency of responses and to answer on the spot in case of any queries. Each

participant independently completed the 60-item inventory, translated into English by specialized staff, with items designed to assess personality traits along the dimensions of the Big Five model. Participants rated the statements on a Likert scale from 1 (strongly disagree) to 5 (strongly agree), which was then transformed into raw scores for each meta-factor and factor. To standardize the results, raw scores were converted to *T-scores*, a psychometric method that allows normative interpretation of individual scores in relation to a larger population. The database (Soto and John 2017a, 117-143) to which the results were compared is shown in Table 1.

TABLE NO. 1

Descriptive statistics for BFI – 2

	Internet sample				Student sample				
Domain or facet	Men *M* (*SD*)	Women *M* (*SD*)	Combined *M* (*SD*)	Gender *d*	Men *M* (*SD*)	Women *M* (*SD*)	Combined *M* (*SD*)	Gender *d*	Sample *d*
Extraversion	3.15 (.78)	3.31 (.80)	3.23 (.80)	.21	3.20 (.70)	3.31 (.73)	3.25 (.71)	.15	−.03
Sociability	2.80 (1.02)	3.10 (1.07)	2.95 (1.05)	.29	2.94 (.86)	3.06 (1.01)	3.00 (.94)	.12	−.05
Assertiveness	3.28 (.92)	3.28 (.93)	3.28 (.93)	.01	3.27 (.82)	3.28 (.85)	3.28 (.84)	.02	.01
Energy Level	3.37 (.88)	3.56 (.89)	3.47 (.89)	.22	3.40 (.80)	3.58 (.72)	3.49 (.77)	.24	−.03
Agreeableness	3.57 (.65)	3.79 (.60)	3.68 (.64)	.35	3.51 (.63)	3.82 (.56)	3.66 (.62)	.53	.03
Compassion	3.72 (.79)	3.97 (.76)	3.84 (.78)	.33	3.60 (.81)	3.98 (.69)	3.79 (.78)	.49	.07
Respectfulness	3.87 (.73)	4.08 (.68)	3.98 (.71)	.30	3.76 (.68)	4.05 (.64)	3.91 (.68)	.44	.10
Trust	3.13 (.83)	3.32 (.80)	3.23 (.82)	.24	3.15 (.77)	3.43 (.77)	3.29 (.78)	.36	−.08
Conscientiousness	3.35 (.74)	3.50 (.79)	3.43 (.77)	.20	3.34 (.60)	3.54 (.66)	3.44 (.64)	.31	−.03
Organization	3.33 (.99)	3.51 (1.03)	3.42 (1.01)	.19	3.46 (.88)	3.68 (.87)	3.57 (.88)	.26	−.16
Productiveness	3.31 (.87)	3.43 (.93)	3.37 (.90)	.13	3.24 (.75)	3.39 (.80)	3.32 (.78)	.19	.07
Responsibility	3.40 (.78)	3.57 (.83)	3.48 (.81)	.20	3.33 (.60)	3.55 (.71)	3.44 (.66)	.33	.05
Negative Emotionality	2.95 (.88)	3.18 (.84)	3.07 (.87)	.27	2.84 (.74)	2.95 (.79)	2.89 (.76)	.14	.21
Anxiety	3.28 (.95)	3.58 (.88)	3.43 (.93)	.33	3.20 (.78)	3.53 (.85)	3.37 (.83)	.40	.07
Depression	2.82 (1.03)	2.88 (1.02)	2.85 (1.02)	.06	2.65 (.92)	2.53 (.93)	2.59 (.93)	−.14	.26
Emotional Volatility	2.77 (1.04)	3.09 (1.04)	2.93 (1.05)	.31	2.66 (.91)	2.79 (.97)	2.73 (.95)	.13	.20
Open-Mindedness	3.93 (.64)	3.91 (.67)	3.92 (.65)	−.02	3.71 (.65)	3.62 (.63)	3.66 (.64)	−.15	.39
Intellectual Curiosity	4.18 (.69)	4.03 (.71)	4.10 (.70)	−.21	3.89 (.76)	3.80 (.70)	3.85 (.73)	−.12	.24
Aesthetic Sensitivity	3.71 (.90)	3.88 (.94)	3.80 (.92)	.19	3.57 (.95)	3.58 (.90)	3.58 (.92)	.02	.36
Creative Imagination	3.89 (.81)	3.82 (.80)	3.85 (.81)	−.09	3.68 (.75)	3.46 (.77)	3.57 (.77)	−.28	.36
Sample size	500	500	1,000		313	146	459		

All results were manually entered into a common database, which was analyzed to obtain data on the total mean of each trait, the standard deviation of the responses, the mean of the first-year subgroup, the mean of the second-year subgroup, and the total.

A personality trait profile was compiled for each subject, as exemplified in Tables 2 and 3.

TABLE NO. 2

Full profile of subject 10 (S10) by *T – score*

	Mean	*T-score**
Extraversion	4.0	61.4
Sociability	3.5	56.5
Assertiveness	4.0	58.9
Energy Level	4.5	63.8
Agreeableness	3.6	51.2
Compassion	3.8	51.9
Respectfulness	3.8	49.9
Trust	3.3	51.3
Conscientiousness	4.3	65.2
Organization	4.3	59.0
Productiveness	4.0	60.1
Responsibility	4.5	69.5
Negative Emotionality	2.4	44.3
Anxiety	3.3	50.6
Depression	1.8	40.2
Emotional Volatility	2.3	45.5
Open-Mindedness	3.4	45.5
Intellectual Curiosity	3.8	48.2
Aesthetic Sensitivity	2.3	36.1
Creative Imagination	4.3	57.6

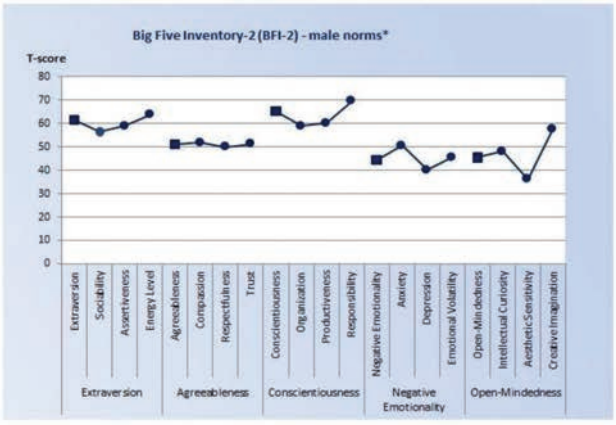
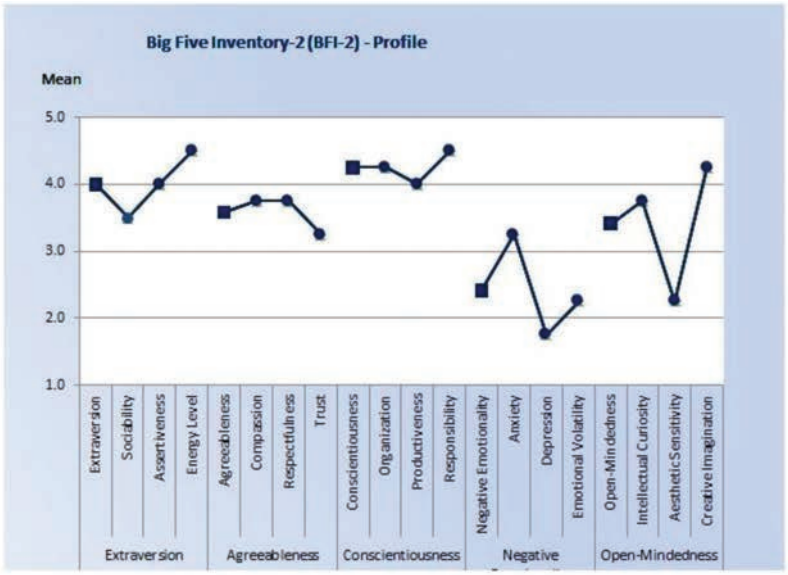


TABLE NO. 3

BFI – 2 profile of subject 10 (S10)



Data analysis

The data were analyzed by calculating the mean *T-scores* for each factor for each subject, then compared with normative data to determine the degree of deviation. Descriptive statistics were used to identify the personality profiles of the sample, with particular attention paid to high or low scores relative to the normative mean. This methodological approach ensures that the study results are both statistically valid and applicable in a controlled leadership context. The use of *T-score* and factor-level analysis provided by the BFI-2 contribute to a detailed understanding of personality profiles.

TABLE NO. 4

BFI - 2 results for the first subgroup

Extraversion	57.9	54.3	69.8	59.0	46.0	63.8	54.3	56.7	50.7	52.6	53.7	56.7	44.6	54.3	56.7
Sociability	68.1	56.5	74.0	56.5	50.7	65.2	56.5	56.5	56.5	51.9	51.9	59.4	49.4	53.6	56.5
Assertiveness	43.7	46.7	62.0	58.9	43.7	62.0	52.8	52.8	46.7	58.5	52.6	55.9	46.7	52.8	55.9
Energy Level	57.5	57.5	63.8	57.5	45.0	57.5	51.3	57.5	48.1	45.4	55.8	51.3	38.5	54.4	54.4
Agreeableness	60.4	56.5	71.0	52.5	45.9	67.0	56.5	56.5	51.2	53.2	50.2	53.8	48.8	55.1	51.2
Compassion	58.0	51.9	67.3	48.8	45.7	64.2	54.9	51.9	48.8	53.9	50.3	48.8	43.0	51.9	45.7
Respectfulness	53.5	53.5	60.9	46.2	46.2	64.6	53.5	53.5	53.5	49.2	49.2	53.5	37.5	53.5	57.2
Trust	64.3	61.0	74.0	61.0	48.1	64.3	57.8	61.0	51.3	54.2	50.9	57.8	63.9	57.8	51.3
Conscientiousness	61.0	54.1	77.7	66.6	45.7	67.9	66.6	58.2	61.0	57.0	62.0	49.9	40.6	62.4	63.8
Organization	53.3	47.6	67.5	61.8	47.6	67.5	59.0	53.3	56.1	53.7	56.6	50.5	39.3	59.0	59.0
Productiveness	66.8	60.1	73.5	66.8	46.8	66.8	66.8	56.8	60.1	57.6	60.8	50.1	42.0	60.1	60.1
Responsibility	57.0	52.8	77.8	61.2	44.5	57.0	65.3	61.2	61.2	56.3	63.4	48.7	45.8	61.2	65.3
Negative Emotionality	46.5	47.7	26.3	45.4	46.5	37.5	34.1	47.7	44.3	40.1	40.1	46.5	50.6	45.4	44.3
Anxiety	41.0	47.4	25.0	50.6	44.2	28.2	34.6	44.2	41.0	37.9	37.9	47.4	52.6	44.2	37.8
Depression	51.1	48.4	32.1	37.5	51.1	45.7	37.5	48.4	48.4	44.3	47.0	45.7	52.4	48.4	45.7
Emotional Volatility	48.2	48.2	31.8	51.0	45.5	42.7	37.3	51.0	45.5	41.9	39.3	48.2	47.0	45.5	51.0
Open-Mindedness	51.9	44.2	59.6	46.8	44.2	46.8	42.9	37.8	41.6	54.7	57.4	50.6	46.8	48.1	48.1
Intellectual Curiosity	48.2	44.9	48.2	44.9	44.9	51.4	35.0	38.3	44.9	49.3	56.4	44.9	49.3	48.2	44.9
Aesthetic Sensitivity	51.9	44.0	57.2	49.3	44.0	36.1	44.0	38.7	41.4	51.9	54.7	51.9	43.6	46.6	46.6
Creative Imagination	54.3	47.6	67.6	47.6	47.6	57.6	54.3	44.3	44.3	60.3	57.0	54.3	50.5	50.9	54.3
	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24	S25	S26	S27	S28	S29

The use of the T-score was essential to this study because it allowed comparison between the study sample and a normative population as the T-score standardizes scores around a mean of 50 with a standard deviation of 10, allowing researchers to determine how well the level of an individual trait relates to the norm. In the context of this study, the T-score provided insights into traits that were more pronounced or diminished among higher-performing leaders compared to benchmarks of the general population. The database resulting from the centralization of the responses was made for the statistical analysis of the subgroups as presented in Tables 4 and 5.

TABLE NO. 5

BFI - 2 results for the second subgroup

Extraversion	65.0	57.9	61.4	54.3	54.3	54.3	59.0	59.5	50.7	61.4	49.5	63.8	57.9	55.5
Sociability	65.2	56.5	59.4	47.8	47.8	53.6	62.3	59.3	53.6	56.5	47.8	62.3	62.3	50.7
Assertiveness	58.9	55.9	52.8	52.8	55.9	52.8	58.9	55.5	49.8	58.9	49.8	62.0	52.8	52.8
Energy Level	63.8	57.5	66.9	60.6	57.5	54.4	51.3	59.3	48.1	63.8	51.3	60.6	54.4	60.6
Agreeableness	52.5	40.6	67.0	55.1	44.6	56.5	53.8	50.2	52.5	51.2	57.8	63.1	55.1	57.8
Compassion	42.6	33.3	54.9	48.8	45.7	54.9	61.1	50.3	54.9	51.9	48.8	64.2	61.1	58.0
Respectfulness	53.5	38.8	64.6	53.5	38.8	53.5	46.2	49.2	42.5	49.9	53.5	53.5	49.9	53.5
Trust	61.0	54.5	74.0	61.0	51.3	57.8	51.3	50.9	57.8	51.3	67.5	64.3	51.3	57.8
Conscientiousness	70.7	63.8	76.3	61.0	63.8	45.7	55.4	63.3	61.0	65.2	69.3	69.3	48.5	62.4
Organization	64.7	64.7	67.5	56.1	59.0	36.3	53.3	56.6	59.0	59.0	59.0	56.1	41.9	56.1
Productiveness	66.8	56.8	73.5	60.1	60.1	53.5	56.8	63.9	60.1	60.1	66.8	66.8	56.8	63.5
Responsibility	69.5	61.2	73.7	61.2	65.3	52.8	52.8	63.4	57.0	69.5	73.7	77.8	48.7	61.2
Negative Emotionality	38.6	40.9	38.6	40.9	46.5	36.4	42.0	36.9	39.8	44.3	39.8	27.4	47.7	37.5
Anxiety	50.6	47.4	41.0	37.8	41.0	37.8	37.8	34.9	34.6	50.6	31.4	28.2	50.6	34.6
Depression	37.5	34.8	40.2	45.7	42.9	37.5	48.4	38.9	48.4	40.2	42.9	32.1	48.4	42.9
Emotional Volatility	34.5	45.5	40.0	42.7	56.5	40.0	42.7	41.9	40.0	45.5	48.2	31.8	45.5	40.0
Open-Mindedness	45.5	46.8	45.5	45.5	48.1	36.5	54.5	53.4	57.0	45.5	44.2	55.7	41.6	49.3
Intellectual Curiosity	48.2	35.0	48.2	51.4	44.9	28.4	48.2	49.3	58.0	48.2	44.9	54.7	31.7	44.9
Aesthetic Sensitivity	38.7	44.0	33.5	38.7	54.5	41.4	51.9	51.9	51.9	36.1	41.4	57.2	41.4	49.3
Creative Imagination	54.3	64.3	60.9	50.9	44.3	47.6	60.9	57.0	57.6	57.6	50.9	50.9	57.6	54.3
	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14

Given that the study group consists of a small number of subjects (< 30) the results obtained were compared to the sample presented in Table 1, and Table 6 presents the final average obtained.

TABLE NO. 6

Average BFI-2 results

Extraversion	56.4	57.5	55.4
Sociability	56.8	56.1	57.6
Assertiveness	53.8	55.0	52.8
Energy Level	55.4	57.9	53.0
Agreeableness	54.7	54.1	55.3
Compassion	52.3	52.2	52.3
Respectfulness	51.3	50.1	52.4
Trust	58.3	58.0	58.6
Conscientiousness	61.0	62.6	59.6
Organization	55.9	56.4	55.4
Productiveness	60.7	61.8	59.7
Responsibility	60.9	63.4	58.6
Negative Emotionality	41.4	39.8	42.9
Anxiety	40.4	39.9	41.0
Depression	43.6	41.5	45.6
Emotional Volatility	43.8	42.5	44.9
Open-Mindedness	47.9	47.8	48.1
Intellectual Curiosity	45.8	45.4	46.2
Aesthetic Sensitivity	46.0	45.1	46.8
Creative Imagination	53.8	54.9	52.8
	Media	An 2	An 1

Data interpretation

Each of the Big Five Meta – Factors: *Extraversion, Agreeableness, Conscientiousness, Emotional Instability* and *Openness to Experiences* was examined in detail, Table 1 shows the mean T-scores for the five Meta-Factors, highlighting high scores (maximum green, minimum red) for *Conscientiousness* and *Emotional Stability* and moderate scores for

Extraversion and *Agreeableness*. These findings suggest a personality profile aligned with characteristics essential for effective leadership.

To classify the results obtained, I used the following scale defined by a standard deviation of 10: T-scores in the range of 20–34.99 are considered very low; T-scores in the range of 35–44.99 are considered low; T-scores in the range of 45–55 are considered average; T-scores in the range of 56.1–65.99 are considered high; and T-scores in the range of 66–80 are considered very high.

The mean *T-score* for *extraversion* (56.4) indicates a moderate level of sociability and energy among the sample. Subjects within the study group scored high on the *Sociability* (56.8) and *Energy level* (55.4) factors, suggesting a natural inclination toward positive interactions with others and a consistent enthusiasm within groups. These factors are beneficial in leadership as they contribute to a leader's ability to raise the morale of a team and maintain an optimistic attitude, which can be instrumental in motivating team members. The *T-score* for *Assertiveness* (53.8), although moderate, reflects a reserved tendency to impose one's decision-making power on others, suggesting leadership that balances authority with approachability. This balance in *assertiveness* supports a leadership style that commands respect without overwhelming subordinates, a characteristic often associated with effective leadership (Judge et al. 2002, 765-780).

With a mean *T-score* of 54.7, *Agreeableness*, among the study group, is moderately high. *Trust* stands out with a high *T-score* (58.3), indicating that these leaders are generally inclined to view the world around them positively, a trait that facilitates cooperative relationships and trust-building within the team. This attitude is valuable in military contexts that are based on mutual respect and cohesion, where trust in the commander is essential, making the difference between a commander and a commander who is also a leader. *Compassion* (52.3) and *Respect* (51.3) scored moderately high, indicating that while these leaders display empathy, they do so in a balanced way that does not compromise assertive decision-making. This profile aligns with research suggesting that moderate levels of agreeableness enhance team dynamics and cooperation without impairing a leader's ability to act decisively (Graziano and Eisenberg 1997).

Conscientiousness emerged as the most pronounced trait among the study group with a mean *T-score* of 61.0, marking it as a defining characteristic of the sample. Within this Meta-factor, *Productivity* (60.7) and *Accountability* (60.9) scored the highest, emphasizing a strong commitment to perform tasks effectively. This high level of *conscientiousness* is consistent with previous findings suggesting that *conscientiousness* is a significant predictor of job performance, particularly in roles that require organization, attention to detail, and responsibility (Barrick and Mount 1991). The *Organizing* factor, with a *T-score* of 55.9, reinforces the profile of a leader who values structure and meticulous planning, traits essential for managing

complex tasks and maintaining consistent performance under pressure. Overall, the high scores on the *Conscientiousness* domain factors underscore the goal-oriented tendencies of the leaders in this sample, mission–oriented and disciplined individuals who have sworn a sacred oath to defend their country... even at the cost of their lives.

The low mean *T-score* in *Negative Emotionality* (41.4) indicates that the leaders in this sample exhibit high levels of emotional stability. *Anxiety* (40.4) and *Emotional Volatility* (43.8) were particularly low, suggesting that these leaders possess a strong emotional balance, a trait essential for maintaining composure in critical situations. Low scores on *Depression* (43.6) also indicate a stable state of mind, essential for good decision-making and performance. This stability aligns with findings from leadership psychology that link low *Neuroticism* or *Emotional Instability* with effective stress management and a stable attitude in the face of adversity (Watson and Clark 1994). The low overall scores on the *Negative Emotionality* factors suggest that leaders in this sample are less prone to emotional disturbances, thus favouring an effective and calm leadership style suitable for crisis-resolution environments such as the military.

Openness to Experiences had a moderate mean *T-score* of 47.9, indicating an openness to new experiences, balanced by a preference for conservative and practical approaches. Of the factors, *Creative Imagination* had the highest score, 53.8 suggesting that although these leaders are capable of innovative thinking, their creativity is applied in a stable and strategic manner. In contrast, *Intellectual Curiosity* (45.8) and *Aesthetic Sensitivity* (46.0) were slightly below the population average, suggesting an emphasis on concrete, results-oriented goals, operating from standard procedures rather than abstract or artistic interests. This pattern of moderate openness broadly aligns with the military system's approach to innovation, where adaptability is valued within the confines of practical, mission–centred goals. The leaders in this sample demonstrate a balanced approach between embracing novelty and strictly applying procedures, an advantage in areas that require the strategic application of creativity.

T-score analysis reveals a personality profile compatible with leadership characterized by high *conscientiousness* and *emotional stability*, moderate *extraversion* and *agreeableness*, and a balanced *openness to experiences*. High scores on *Conscientiousness* factors such as *Productivity* and *Responsibility* emphasize the disciplined and goal-oriented approach of these leaders. Low scores on emotional instability emphasize their ability to remain disciplined and resilient, which are essential for maintaining performance in stressful environments. Moderate levels of *Extraversion* and *Agreeableness* facilitate positive team interactions and confidence building, without compromising decisiveness. Together, these traits suggest a leadership profile that balances an emphasis on task accomplishment with interpersonal skills.

Due to the limitations of this study, the results obtained cannot represent a generalization generating conclusions at the level of the entire category (delimitation) of officers in the Romanian Air Force due to the impossibility of forming a representative sample, some data on the number and command experience of officers having a classified character. Another limitation that I could not control is related to the degree of honesty of the subjects, as well as the correct understanding of the questions that constituted the administered forms even though I was available for clarifications during the completion of the tests. Another limitation of the study may be represented by the sample to which the data obtained in calculating the *T - T-score*, the conclusions and the description of the factors and meta-factors imply the description of a group of individuals compared to the general population, the situations in which the act of leadership is exercised may imply variables that have not been taken into account.

Conclusions

High *T-scores* on *Conscientiousness*, particularly on factors such as *Productivity* and *Accountability*, indicate a goal-oriented, disciplined, and detail-oriented approach among military leaders. High *conscientiousness* is consistently associated with job performance in leadership research, implying a sustained effort in accomplishing tasks, leaders who exhibit high *conscientiousness* are often able to maintain a structured environment essential for clear decision-making and goal achievement in complex assignments. This study reinforces the idea that conscientiousness, with its associated factors, is not only a predictor of goal–oriented success but also a foundation for cultivating the organizational skills that leaders need.

Low *T-scores* on *Emotional Stability*, particularly on *Anxiety* and *Emotional Volatility*, suggest a high degree of emotional stability, an essential leadership trait. *Emotional stability* enables leaders to manage stress effectively, maintain composure, and make informed decisions unaffected by external factors or internal disturbances. Findings demonstrate that the emotional stability of high-performing leaders is important for both individual resilience and team trustworthiness, as leaders who exhibit a calm and steady demeanour are more likely to inspire trust and reliability within their teams. Thus, emotional stability emerges as an essential trait for leadership success.

Future research could also investigate cultural differences in the manifestation of these traits, as the impact of personality on leadership may vary by cultural context. Cross-cultural studies examining BFI-2 profiles of leaders in diverse cultural contexts could reveal how certain traits are valued, contributing to a more nuanced understanding of the role of personality in global leadership.

References

Barrick, M.R., and M.K. Mount. 1991. "The Big Five Personality Dimensions and Job Performance: A Meta-Analysis." *Personnel Psychology* 44 (1): pp. 1-26.

Bono, J.E., and T.A. Judge. 2004. "Personality and Transformational and Transactional Leadership: A Meta-Analysis." *Journal of Applied Psychology* 89 (5): pp. 901-910.

Graziano, W.G., and N. Eisenberg. 1997. "Agreeableness: A Dimension of Personality." In *Handbook of Personality Psychology*, by R. Hogan, J.A. Johnson and S.R. Briggs (Eds.), pp. 795-824. Academic Press.

Hawkins, P. 2014. *Leadership Team Coaching in Practice: Developing High-Performing Teams.* London: Kogan Page.

Hutton, D.M. 2018. "Critical Factors Explaining the Leadership Performance of High-Performing Principals." *International Journal of Leadership in Education* (Taylor & Francis) 21 (2): 150-170.

Judge, T.A., J.E. Bono, R. Ilies, and M.W. Gerhardt. 2002. "Personality and Leadership: A Qualitative and Quantitative Review. Journal of Applied Psychology." 87 (4): pp. 765-780.

Singh, S. 2003. *Leadership in High-Performing Organisations. In Leadership: Value Based Management for Indian Organisations.* pp. 150-160. AKWL Publications.

Soto, C. J., and O.P. John. 2017a. "The Next Big Five Inventory (BFI-2): Developing and Assessing a Hierarchical Model With 15 Facets to Enhance Bandwidth, Fidelity, and Predictive Power." *Journal of Personality and Social Psychology* 113 (1): pp. 117–143.

___. 2017b. "Short and Extra-Short Forms of the Big Five Inventory–2: The BFI-2-S and BFI-2-XS." *Journal of Research in Personality* 68: pp. 69-81.

Srivastava, S., O.P. John, S.D. Gosling, and J. Potter. 2003. "Development of personality in early and middle adulthood: Set like plaster or persistent change?" *Journal of Personality and Social Psychology* 84 (5): pp.1041–1053. https://doi.org/10.1037/0022-3514.84.5.1041.

Watson, D., and L.A. Clark. 1994. "Emotions, Moods, and Traits." *Journal of Personality and Social Psychology* 67 (3): pp. 486-498.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Tenchi warfare – modern military operations based on the "tenchijin" philosophy

Captain (Nv) (r) Sorin TOPOR, Ph.D.*

*Cyber security expert, National Institute for Research and Development in Informatics – ICI Bucharest/Associate member of the Romanian Academy of Scientists
e-mail: sorin.topor@ici.ro

Abstract

In the context of the ongoing conflict in Ukraine, the protection of material and human resources is an essential condition for regional security. The paper examines a number of trends in technological development, lessons learned from this conflict, and opportunities for applying the Japanese tenchijin philosophy to modern military operations. We propose that under the name of "Tenchi warfare" we highlight the role of advanced military technologies in military operations, with an emphasis on the exploitation of obscure spaces and knowledge, to ensure strong decision-making support in order to synchronize the rhythm of the engaged forces with the rhythm of enemy evolution. Similar to how ninja fighters approach combat, we believe such a strategy could be useful in offensive reactions in various domains, as well as for enhancing national and regional security.

Keywords:
Ukraine conflict; advanced technologies; tenchijin philosophy; tenchi devices; tenchi warfare; national security; military operations.

Article info
Received: 11 November 2024; Revised: 29 November 2024; Accepted: 2 December 2024; Available online: 17 January 2025

Citation: Topor, S. 2024. "Tenchi warfare – modern military operations based on the "tenchijin" philosophy". *Bulletin of "Carol I" National Defence University*, 13(4): 206-220. https://doi.org/10.53477/2284-9378-24-59

The Ukraine conflict has put humanity in front of military operations that can no longer be included in the provisions of the traditional laws of war and other related international conventions. Even if in this space there are destructive strikes on infrastructure elements, by both actors involved, after more than two years there is no declaration of war. Moreover, based on the Internet, extensive propaganda, cyber-attacks, and deep-fake campaigns are carried out with the role of forming and stimulating some opinion trends, which support an ideology, a policy, or something else that will attract sponsors, which can be governments, military-political organizations, NGOs, associations, etc.

In this context, emerging and disruptive technologies hold the most important position, being implemented in weapon systems and other military equipment, but also in systems intended for monitoring and management of regional and international security. The lessons learned from Ukraine allow for the formulation of general observations that compete with the reality that in order for an actor to be able to maintain its dominant strategic position in a certain field, it will have to use advanced technology, which mainly allows it to effectively exploit information resources.

Based on the study conducted, we believe that the identification of obscure elements in various strategic fields, by exploiting information resources, in addition to knowing the adversary, understanding his intentions, hiding his own strategic and operational directions, etc., favors approaches that surprise the adversary, hitting his weak points, with limited resource consumption. By appealing to the Japanese "tenchijin" philosophy and using ML/AI algorithms the rhythm of the military operation can be harmonized with that of the adversary. Similar to ninja tactics, it is observed that a slower rhythm can sometimes lead to the creation of obscure spaces that favor the execution of an attack and surprise the opponent in positions or areas over which, at the respective moment, he cannot achieve effective governance, his attention being focused on other operational elements.

About the japanese "tenchijin" philisophy and some methods of application

The "tenchijin" philosophy was the basis of the training of ninja fighters in ancient Japan and China. The origin of the concept comes from Japanese philosophy, which was inspired by the Chinese archetypal definition and has in its composition the three elements of the structure of the universe: Heaven (or air/ sky meaning "ten"), Earth (or the ground/ the soil under feet meaning "chi") and Man (or human/ mankind meaning "jin"). It symbolizes the balance and unity between the various elements of the universe and can be associated with the concepts of "yin" and "yang", which reflect the duality and interdependence between the different aspects of existence. Coming from the earliest times, when people practiced agriculture and animal breeding, life was sustained by knowing the influences of the smooth rotation of

the four seasons. This rhythm influenced production, belief, and politics. The crisis solution which could lead to war, was strictly determined by when the conditions of the sky, the earth, and human activities were aligned.

Thus, it became a principle of government and military strategies, being formalized and described by the famous military strategist Sun Tzu, in his work, "The Art of War". The strategy of "fighting without fighting" described by Sun Tzu is based on ways of using techniques to avoid direct contact where the opponent is strong and aware, by actions designed to disorient him, desensitize him and, most importantly, the attack should be carried out in ways that the enemy does not expect (Tzu 2026, ch. 8). For this, the three elements are applied on three levels (long, medium and close), from the 8 cardinal directions. Heaven represents the higher position that establishes order. Observance of heavenly orders ensures life (adaptation to the heavenly way means growth). Earth represents the lower position characterized by strength and power. If there is strong will there will be peace. Man holds the middle position. Therefore, all human activities must be performed according to correct rules and in harmony.

The practice of martial arts is based on the wisdom and cognitive power of the practitioner. The training of a ninja fighter was not limited to the practice of fighting techniques but also involved the development of knowledge in astrology and the cosmos, geography, and meteorology. All this knowledge allowed him to understand his position in space in relation to the opponent and how to place himself in relation to him. His disguise methods were an extension of this knowledge. A ninja was prepared to play various roles, having an appropriate outfit, using a language particular to the role performed, as well as a specific behavior that would allow him to complete the mission. Apart from understanding the conditions of space, it was especially important to frame his action in time. The ninja fighter could sense when the opponent's focus changed. Depending on this, he would adopt a slow rhythm, to induce confusion and not be synchronized with the opponent's rhythm.

To complete the counter-attack, an essential condition is to get back in the opponent's rhythm synchronization. His movement will be quick and successive, having the advantage of hitting from the not visible space by the opponent. It can be direct or indirect for added confusion. In addition, the ninja fighter can identify new vulnerabilities in the opponent's defense system, which inevitably arise due to his movement in the attack.
Thus, the ninja fighter meets an attack with various shirks and counterattacks. To become invisible, he understood when to use the smoke grenade and which direction to shirk when the opponent's sword struck. He understood that the arm holding the sword would cover the attacker's eyes, especially if he struck from up to down.

The Japanese dictionary suggests, metaphorically, that this technique represents „going in search of freedom" (Goo 2024). Developing this art of fighting, the

whole Sun Tzu's thesis shows how an opponent can be attracted into an illusion based on deception. The basic condition is that the one who exploits this science has the advantage of knowing and understanding the adversary's vulnerabilities. In the required situation, the opponent's sensory elements are directly hit (for a ninja, damage to the opponent's eyes creates the opportunity to reach unattended spaces).

Creating invisible spaces for the opponent is a strategy that increases the chance and safety of one's own action. If the opponent's attention is focused on the suggested place, his perception of reality is distorted. In an extremely simple way, we appreciate that the strategy of conflict based on the tenchijin philosophy is the art of using obscure spaces and adapting the rhythm so that an action is effective in accordance with the planned objective.

Generalizing, we note that martial arts practitioners do not openly manifest their attack intentions. They have the ability to exploit atypical environments and spaces, eccentric to their relational system. Thus, allowing an opponent to be focused on an illusion will place them in a disadvantageous zone for the opponent. Starting from these principles, applications have been developed in numerous fields, such as medicine, economy, politics, urban planning, security, etc. Even in the field of entertainment, all „magicians", in their performances, use obscure spaces and shift the audience's attention to another movement, achieving tricks in which objects disappear or appear.

Currently, many economic entities in Japan are exploiting these techniques based on the use of spatial information, in order to estimate obscure spaces and land evaluation. These applications are said to be useful in agriculture, fishing, real estate, energy, logistics, tourism (Jaxa 2019), etc. For example, based on the GIS service and using machine learning algorithms (ML/AI), the risks of leaking water pipes can be managed (Tokyo SME 2023). Yasutoshi Hyakusoku, co-founder of the Start-up „Tenchijin" and head of the R&D office/ JAXA (Japan Aerospace Exploration Agency) states that if it has been shown that a large part of economic problems can be solved by technology, there are also social challenges whose solution, even if it is not easy, could be solved in this way, both globally and locally. Hyakusoku believes that „sensors or telecommunications equipment from space that observes the Earth should be part of the planet's infrastructure" (Spotlight 2023).

Within business ecosystems, corporations are increasingly facing cyber-attacks, especially in their relationships with third-party partners and suppliers. Innovative and disruptive solutions are used for cyber risk management in order to provide cyber security services. Endeavor's Scale Up Outliers program (Tenchi 2024) aims to reduce information asymmetry in information security and compliance risks in corporate ecosystems in a cooperative and scalable manner to return on invested capital. Even though these developments have advanced many fields, leading end-to-end cybersecurity services focused on protection strategies, resilience and a range of

industry-specific services have also attracted the attention of some armies, especially in the cloud environment and the organization's ecosystem governance domains.

Being an extremely important field, there is no public information about these services, in which case, our analysis will be limited to tenchijin philosophy approach principles and the effective use of emerging and disruptive technologies. These, having a huge potential to contribute to public security, can always become targets in various attacks, in the context of the existence of a variety of military interventions in the world, but also in other types of international relations.

Advances technologies in the russo-ukrainian war

In the history of humanity, especially in periods of changes in the balance of power of the international order, many conflicts are present. Russia's aggression against Ukraine is a violation of all the rules, and the danger of this pattern is determined by the possibility of a similar situation occurring anywhere in the world. Thus, the risks to regional and global security, on the background of increasing pressures to change the status quo by military force, are complex and increasingly hybrid and can be amplified by the proximity of a country that has a strong army, nuclear weapons, and a real industry of war.

Looking at the current geopolitical context, it is observed that the "frozen wars" and "gray zone" situations of some territories, the expansion of other "gray zones" of postmodern war, combined with transboundary cyber-attacks on critical infrastructures, information controlled, propaganda and deep-fake etc., dilutes the power of the recognized norms between the state of war and those of peace. Domains of national security, previously considered non-military, have been expanded into economic and technological directions. These approaches result in making it excessively difficult to draw the line between military and non-military conflict.

The irony regarding the current state of international security is that all the unprecedented measures and sanctions taken against Russia, even if they aimed to oblige to stop fighting, risk increasing material destruction, increasing the number of victims, and the duration of the conflict. In addition, the confrontations between regimes (Democratic vs. Autocratic), the blending of military and political components, the struggle to obtain dominance in any domains, etc., created uncertainty in establishing the responsibility of the aggressor, in the event of the war starting. Cross-border incidents, missile and drone strikes, sabotage and incursions, destruction and loss of human life, etc., especially following Ukraine's incursion into Russian territory, have heightened regional tensions and created the conditions for a long-term war, with new, associated risks.
These unprecedented military operations could not be possible without the use of advanced technologies, which revolutionized the entire military ecosystem, and influenced the strategies and battles.

We present the main advanced technologies used in the conflict in Ukraine:

A. Drones. Before the beginning of the Russian special operation against Ukraine, even the biggest supporters of the promotion of unmanned aerial systems (UVS) could not have estimated the extent and diversity of the fields of exploitation of drones. After only two and a half years of war, the use of drones is essential for precision strikes and tactical reconnaissance/observation. Drones are capable of operating in information networks based on satellite systems, terrestrial communications networks, and human agents (HUMINT). The information on these devices allowed the rapid assessment of the tactical and operational situation. Thus, against Russian drones, the Ukrainians use miniaturized "tenchi" devices and portable electronic warfare systems. Russia's response was to launch attacks by Lancet kamikaze drones that recognize the target recognition signals, generated by Orlan-10 and SuperCam drones, in the visual and infrared spectrum (Battersby 2024). With this equipment, Russia sought to match the performance of Ukrainian strikes with HIMARS systems (provided by the US) (Farrell 2023), against artillery, tanks, and other high-value targets.

B. Electronic warfare (EW). Due to the particularities determined by the mobility and the increased requirements of information exchange, ensuring the security of the resource of electromagnetic frequencies, attacking the similar resource of the adversary is a main objective of contemporary military operations. Through electromagnetic waves, the coordination and synchronization of actions are achieved, the public's right to information and social communication links are ensured, and the security of critical infrastructures and the protection of the civilian population in the geographical areas related to the conflict are maintained. In this context, electronic warfare equipment is essential for disrupting the adversary's communications, hindering coordination, and disrupting the efficiency of his actions, in an environment where the limits of the electromagnetic frequency spectrum cannot be expanded. Thus, electronic warfare has moved from the stage of active networking to that of active confrontation, constituting a condition for winning and maintaining the initiative.

The Russians, unlike NATO countries, have operationalized electronic warfare at all hierarchical levels (strategic, operational, and tactical) and in all components of its army (land, sea, air, and space). EW forms the basis of information warfare doctrine (Chiriac and Withingon 2024). In fact, David T. Pyne, a researcher at the EMP Task Force and former director of the US Department of Defense, estimates that Russia has "the most capable electronic warfare system in the world" (Giangiulio 2023), being impressed by the speed of adaptation at the performances of latest US and NATO weapons systems.
Russian electronic warfare equipment has been able to render the Excalibur, GLSDB, and HIMARS technologies ineffective by jamming satellite signals (Skove 2024). They disrupted the Starlink Internet capabilities, provided by the Pentagon, complicating the coordination of forces and the launching of Ukrainian drone

strikes (Mozur and Satariano 2024). In this war, Ukraine would not have lasted so long without the support of technology companies from the US, Europe, and Asia who provided high electronic and cyber technology that allowed them to use the weapons systems (Topor 2024).

Moreover, the Ukrainian military forces in the incursion at Kursk (August 2024) benefited from effective EW support, which supported the creation of obscure spaces in the Russian defense. Success would not have been possible without information, timing, and decision support. This military force involved hundreds of Ukrainian troops, infantry units, mechanized units, and drone support. The operational surprise was evident, and the response of Russian forces was far too slow to stop the offensive and push the Ukrainians across the border. Still, electronic warfare should not be confused with cyber warfare and other hacking techniques (NATO 2023) of electronic devices.

C. Cyberwarfare: Cyberwarfare, and especially the cyber defense component, has become a critical component of Ukraine's national security strategy. Cyberspace is recognized as the fifth domain of war, along with land, air, sea, and space (Avanesova, Serhiienko and Lyubushin 2022, 25-40). Mainly, the cyber dimension of warfare is a dominant component in the battle for online information, from campaigns to winning hearts and minds (Willett 2022). In this conflict, cyber warfare can be classified into three levels of approach, namely: destructive cyber-attacks, network penetration for espionage activities, and last but not least, psychological influence operations of the international audience through cyber sociology products. Against it, Ukraine could not have coped with the situation without Western and NATO support.

Through the Internet, the emotions of anyone interested in this event were stimulated by messages guided around key terms such as war, victory, death, destruction, fear, migration, etc. Thus, a semantic space was created for the application of AI/ML search engine algorithms, as well as a series of meta-tags within social networks, as response strategies for the radicalization of the international audience. Thus, alliances of states, coalitions of companies from the public or private sectors, and NGOs were formed, which supported one of the two actors involved. Official and unofficial narratives varied significantly, depending on the source, and accompanied direct contact between the armed forces. Usually, the Russian component characterizes the fighting as a form of defense against terrorism and other highly aggressive provocation movements of Ukraine, as a direct action on national sovereignty, and as a measure to increase security against the nazification of the Russian population by the Ukrainian regime. On the other hand, Ukraine praises the bravery of its armed forces, makes accusations of war crimes, and calls for Western defense support.

Through cyber-attacks, presidential elections were manipulated, energy distribution companies, financial institutions, postal services, news publications, transport and commercial services were hit, government web pages and even telecommunications

services that were provided through the Starlink satellites system were affected. The symbolic value of Ukraine's cyber defense far exceeded the operational value of the military maneuvers, demonstrating the resolve and sustainment of Ukrainian combat capabilities (Youvan 2024).

D. Missile systems and precision artillery. In the field of weapons, advanced technologies have been implemented in strike systems to increase the accuracy of strikes (especially on infrastructures of strategic value), reduce collateral damage, as well as to improve operational efficiency. At the tactical level, the missile and artillery systems used by both actors led to the so-called artillery genocide (70% of Ukrainian casualties are caused by Russian ground artillery), with Ukrainian forces dealing only with self-propelled artillery, received as aid (Buță and Manoliu 2023, 168-175). At the strategic level, Russia's development and use of hypersonic missiles have prompted a review of European and NATO defense and risk assessment strategies, and it is quite possible that Russia might continue to develop appropriate, high-speed, nuclear-extended capabilities (Wright 2022). Although these challenges can be mitigated through international technical and political mechanisms, potential manufacturers can continue to invest in scientific research and technological testing leading to new systems whose performance exceeds current ones.
For example, Ukraine uses Switchblade missiles (v. 300 and 600), a tactical missile-drone-AI combination with autonomous capabilities, ground-launched and autonomous target-locating and systems-priority strike capabilities of anti-aircraft, tank, and other Russian defense systems (Cook 2024).

E. Artificial intelligence (AI). AI algorithms have improved data analysis, mission planning, and resource optimization. Thus, the speed and accuracy of decision-making activities in numerous military and civilian fields have been increased. Military decision-making structures can use AI in operational and tactical fields to predict conflict zones, optimize evacuation routes, or prioritize the treatment of the wounded (Kolesnikov and Kryzhevsky 2023). At a strategic level, AI can be used to support foreign policy decisions and diplomacy (Sirenko 2024, 122-128), manage emergencies, rebuild infrastructures, and even counter disinformation (Kertysova 2018, 55-81). It should be noted that the war in Ukraine has caused a very rapid development of autonomous systems based on AI, the involvement of which has changed the dynamics of combat maneuvers. In addition to drones, EW, intelligence and cyber warfare systems use AI to collect data, spread disinformation (including image and video manipulation), intercept unencrypted communications, geo-locate and analyze open-source data to identify soldiers, weapons, systems, units, and their maneuvers (Marija and Vanja 2023, 59-76). This does not mean that the role of conventional weapons is ignored. The essence of the use of AI in armed conflicts is reflected in the economy of human resources and the reduction of casualties.

F. Secure communications. Advanced communication technologies have improved communication methods to coordinate maneuvers between units and transmit

information quickly and securely. Obviously, digitized technological solutions have provided the opportunity to create new governance systems that have allowed the optimal use of resources, the modernization of policies and specific services, as well as the effective interaction of all structural units, military and civil, at all hierarchical levels. In this regard, data and information protection has become not only a technical but also a legislative issue for the Ukrainian government and beyond. From a technical point of view, the use of Starlink satellites has brought enormous benefits to keeping many communications services intact, especially for forces engaged in warfare. In addition, a number of administrative structures have been created and developed to ensure the security of public services, in electronic forms, such as the iGov.org web portal, the Kiev Tsyfovii application (for using various community services via smartphone), other applications that ensure several functionalities related to the hostilities on the territory of Ukraine (shelter map, map of an ongoing business, voluntary help of the army, voluntary assistance, links to official sources etc.) (Bojor, Petrache and Cristescu 2024, 185-194), strengthening social resilience.

G. Air defense: The war in Ukraine, in addition to drones, has also become a testing theatre for new air defense technologies. These were essential for protecting ground forces from Russian air strikes and missile attacks. In fact, the aspects regarding the modernization of Ukrainian air defense systems have been the subject of many publications, following the whole range of systems, with long, medium, short, and close range of military equipment complexes (Spirin, Pogorilyi and Shynkarenko 2023, 75-81). The new systems included new optoelectronic technologies, for accurately determining the coordinates of the target, for faster detection and reducing the reaction time to changes in the operational situation, electronic attack protection components, mobility and obstacle-overcoming capabilities, etc. Due to the time constraints associated with the deployment and testing of new systems in combat, a number of limitations have also been identified, which are mainly determined by ensuring compatibility with other weapons, communications systems, and drones. On the background of the support of Ukraine by European countries and NATO with modern equipment, Russia could not ensure its air superiority, being forced to change its tactics of using air power, focusing its effort on missile and drone strikes. Unfortunately, the situation of the Russian Federation's lack of control of airstrikes, with cruise missiles and drones, continues to cause many casualties among Ukrainian civilians (Титаренко and Власенко 2024).

H. Education and training technologies: Advanced simulation technologies have enabled effective training, adequate training of soldiers to deal with various combat scenarios, and improvement of their reactions under conditions of stress and uncertainty. Among the many technological innovations intended for military training, we mention virtual multimedia simulators, educational games, automatic knowledge assessment systems, distance learning equipment, etc. The use of these educational tools, in addition to improving the efficiency of training and motivation, also allowed the reduction of time and related costs. This improves applied military

education, the quality of learning materials, and assessment models. This approach aligns with the trend of integrating advanced information technologies into military education, becoming a crucial tool for modernizing military education and training. Effective solutions are provided for the use of sensors, weapons, and other combat systems to meet the evolving needs of the armed forces in the context of ongoing warfare. In addition, these solutions are also useful in raising the morale of Ukrainian troops, supporting the motivation to respond to hybrid threats, training military specialists, and developing skills in the use of weapons, in accordance with NATO standards (Kozubtsov et al. 2023).

Generally, we appreciate that the military operations carried out in this conflict demonstrate the importance of collaboration and coordination of the maneuvers of the components of the armed forces structures, in order to obtain the tactical and operational advantage. This involves synchronization and efficient exchange of information and resources. We estimate that in line with the development of advanced technologies towards digitization and miniaturization, weapon systems and military equipment will be increasingly numerous, more precise, more efficient, and integrated, as the electromagnetic environment and cyberspace will become indispensable for any type of warfare.

Analysis and discussion of "tenchi" military operations

Current advanced technologies favor the production of a multitude of relevant information, analysis, and predictions, which, with appropriate learning and training in order to develop knowledge, can represent the basis of effective management in a diversity of fields. The category of tenchi electronic devices includes smartphones, smart health monitoring devices, smart watches, and other types of portable electronic devices that use big databases and communication networks. All of them contain advanced communication technologies, such as Bluetooth or Wi-Fi, sensors for measuring various parameters (from health to environment), intuitive interfaces, algorithms, and other applications that support human activity. Tenchi devices are also included in industrial machines that, depending on the environment of use, can perform various activities from product packaging to food processing (Tenchi Sangyo Co. 2021).

Conceptually, there is no category of activities that can be identified with this name. „Tenchi warfare" is a screenplay of the animated film „War on Geminar", a spin-off of the Japanese series Tenchi Muyo! We consider that the hypotheses addressed in this film can become reality in the conditions in which disruptive and emerging technologies are increasingly present in everyday life. The video game based on this film puts participants in combat scenarios between samurai and ninja characters with special abilities to navigate complex levels, avoid enemies, eliminate targets, steal information, and rescue hostages, all without being detected. A variety of

weapons, combinations of strategic actions, and stealth tactics lead to the resolve of missions to uncover political conspiracies and avenge betrayals, obviously in the Japanese feudal atmosphere. The game puts players in front of moral choices that can affect the story and relationships with various characters. The multiplayer mode allows players to compete against each other using stealth, camouflage, and disinformation skills.
A game apparently similar to those from the „capture the flag" or „assassination" class, it is quite addictive in digital media. Yet, similarly to other strategic war games, they can form wrong perceptions of the ethical and moral norms of war for a young person with no military training

For military science analysts and researchers, it can be a useful tool to understand some aspects of techijin philosophy. Practicing stealth techniques can develop skills for identifying obscure spaces and a mission rhythm, which can then be practiced in real life in a complex environment with asymmetric and hybrid risks and threats.
It is well known that the notion of cyber warfare was developed around the concept of cyberspace. The paternity goes to the novelist William Gibson who, in his book Neuromancer (1984), established through cyberspace a virtual space, beyond the physical world, accessible through computer networks, having a strong impact on the vision of what the current Internet represents. With the introduction of the Internet into military operations, cyberspace has become a core concept that sets the environment for information warfare, with individuals who can attack and/or determine a high level of security for computers and computer networks (Van Haaster 2019).

Similarly, we define the concept of „tenchi warfare" as those strategies and methods of warfare based on advanced technologies, emerging and disruptive technologies, on the enemy's critical infrastructures, manipulating information, anticipating developments and projecting power, as well as ensuring security against risks and hybrid threats. From an ethical and moral point of view, a big problem is the use of manipulation to destroy a social system, organized around a certain ideology. We pointed out that terrorism and long-range strikes are meant to achieve destruction and loss of human life in warfare that cannot be framed in international law under the concept of war.

Currently, the opportunity to exploit advanced technologies in warfare largely ensures victory. The challenges regarding the protection of critical infrastructures and the civilian population captive to the conflict space are derived not from the use of emerging and disruptive technologies, but from the purpose for which it is used. In this context, we believe that military operations based on the art of tenchijin can be planned and executed, which we include in the concept of „tenchi warfare".
For example, even if the falsity of the Russian motivation regarding the legalization of the war against Ukraine is recognized (Russia invoked maintaining peace in the

Donetsk and Lugansk regions, as well as stopping the genocidal crimes committed in the eastern Donbas region) and determined an international mechanism to establish the perpetrators' crimes during the war, Russia used military force and occupied several critical and strategic Ukrainian locations (Khater 2022). Ukraine's reaction, under intense information warfare and under strikes that include advanced technologies, can be considered a tenchi operation, based on strategies that established a high level of collaboration and effective coordination of forces, adjusting the rhythm of defense operations to the rhythm of the Russian offensive, the execution of offensive counterattacks in areas and with methods that allowed him to surprise the opponent.

No one expected that on August 6, 2024, two and a half years after the start of the war, Ukrainian troops would make a successful incursion into Russian territory, reaching Kursk. Remarkable are the scale and speed of this military operation, the knowledge of the reality of the reaction power of the Russian forces in the defense breach area, as well as the way of preparing the entire military operation, under the umbrella of unprecedented security measures. Thus, Ukraine established a buffer zone to prevent the bombing of its territory in the Kursk region, an additional pressure on Russia (which was obliged to transfer troops from another contact zone to stop the offensive) and an imagological gain, essential in restoring the morale of the troops and civilian population.

Moreover, this strategy allowed the rapid acquisition and maintenance of tactical and operational advantages in numerous areas, among which we enumerate:

1. Exploitation of Russian defensive weaknesses, improved penetration tactics, and combined use of advanced technology, GIS intelligence, drones, sabotage actions, precision strikes, and maneuver strategies;
2. International support with modern equipment and systems, adapting and reforming tactics according to combat capabilities;
3. Improved mobility and attack capabilities focused on the enemy's weak points;
4. Demonstrating the effective use of information capabilities to demoralize Russian troops and mobilizing public opinion to increase national solidarity;
5. Expanding defense and tactical adaptation capabilities depending on the type of battle (urban warfare, open ground warfare, electronic warfare, etc.);
6. The recapturing of territories that allowed a controlled withdrawal from other areas, followed by quick and effective counterattacks.

We appreciate that this incursion can be similar to the counterattack of a ninja who has understood how to use, in his favor, obscure spaces and domains, in the background of an adapted rhythm of strategic defense, followed by a quick offensive reaction, until the moment when the planned objectives are achieved.

Conclusions

In the context of digital transformation and the development of emerging and disruptive technologies, the growing trends of the defense and security equipment market, the implementation of technological advances in increasingly complex systems, and the ability to stimulate scientific research and the production of new equipment, with significant investments in various fields, etc., the proposed concept of "tenchi warfare" can characterize this historical moment in the evolution of military art. Currently, even though many different factors depend on the regional geopolitical and military context, every country is aiming to strengthen its defense capabilities and improve its military training.

The concept presented is a hypothesis of scientific research, resulting from the descriptive analysis of the Japanese philosophical concept, applied to advanced technologies for the military field, based on which, through a series of modeling, simulations, and tests, it can be established how useful it might be in this regard and what the conditions are for its implementation in military operations. Such an approach can be useful both in the phase of establishing the combat platforms design, in the stability of the level of armament, etc., and the stability of strategies for reorganization of combat units.

Moreover, we consider that strategic planning, developed through such an approach, can outline effective directions for the development of the future military industry for strengthening the security of critical infrastructures, with the main requirement being the protection of human resources, in the context of hybrid attacks, supported by an intense information warfare. We estimate that other directions related to the strengthening of national security with a strong positive impact on the national economy can be developed.
Through the multitude of domains addressed, we emphasize that this study is a commitment that our research will continue and the results obtained will be published in future works.

References

Avanesova, N.E., Y.I. Serhiienko, and R.A. Lyubushin. 2022. "Strengthening the State Cyber Defence and Creating of Cyber Troops: State, Problems and Organizational – Economic Measureas for Ukraine." *Economic Innovations* 24 (1): 82. https://doi.org/10.31520/ei.2022.24.1(82).25-40.

Battersby, Blair. 2024. *Russia Struggling to Integrate Its Most Effective Unmanned System, TRADOC G2.* https://oe.tradoc.army.mil/2024/04/18/russia-struggling-to-integrate-its-most-effective-unmanned-system/.

Bojor, Laviniu, Tudorică Petrache, and Cristian Cristescu. 2024. "Emerging Technologies in Conflict: The Impact of Starlink in the Russia-Ukraine War." *Land Forces Academy Review* 29 (2): 185-194. https://doi.org/10.2478/raft-2024-0020.

Buță, Viorel, and Răzvan Manoliu. 2023. "Noi tendințe în întrebuințarea diferitelor arme în războiul Ruso-Ucrainean." *Conferința științifică internațională „Gândirea Militară Românească", Teorie și Artă Militară.* doi:doi.org/10.55535/gmr.2023.4.09.

Chiriac, Olga R., and Thomas Withingon. 2024. *Russian Electronic Warfare: From History to Modern Battlefield, Irregular Warfare Initiative.* https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/.

Cook, Ellie. 2024. "US-Made `Tank-Killer` Switchblade Destroys Russian SAM System in Rare Video." *Newsweek.* https://www.newsweek.com/ukraine-switchblade-drone-russia-tor-air-defense-system-video-1976448.

Farrell, Francis. 2023. *How Russia's homegrown Lancet drone became so feared in Ukraine, The Kyiv Independent.* https://kyivindependent.com/how-russias-homegrown-lancet-drone-became-so-feared-in-ukraine.

Giangiulio, Graziella. 2023. "#UKRAINERUSSIAWAR. For Kiev it is the last chance but Moscow last the numbers to win on paper." *News AGC Communication.* https://www.agcnews.eu/ukrainerussiawar-for-kiev-it-is-the-last-chance-but-moscow-has-the-numbers-to-win-on-paper/.

Goo. 2024. *„Tenchi", [traducere din japoneză].* https://dictionary.goo.ne.jp/srch/jn/%E3%83%86%E3%83%B3%E3%83%81/m0u/.

Jaxa. 2019. "Introduction of JAXA ventures." *Tenchijin, Inc.* https://aerospacebiz.jaxa.jp/en/venture/tenchijin/.

Kertysova, Katarina. 2018. "Artificial Intelligence and Disinformation: How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered." *Security and Human Right* (No.29): 55-81. https://doi.org/10.1163/18750230-02901005.

Khater, Maya. 2022. "The Legality of Russian Military Operations Against Ukraine from the Perspective of International Law." *Access to Justice in Eastern Europe Journal.* doi:10.33327/AJEE-18-5.3-a000315.

Kolesnikov, E.B., and V.V. Kryzhevsky. 2023. "The use of Artificial Intelligence at the Stages of Evacuation, Diagnosis and Treatment of Wounded Soldiers in the War in Ukraine." *Kharkiv Surgical School* (no. 4-5 (September)): 80-83. https://doi.org/10.37699/2308-7005.4-5.2023.11.

Kozubtsov, Igor, Ihor Danyliuk, Andrii Krasnobokyi, and Svitlana Voronaia. 2023. "Prospects for the use of Virtual Reality Technologies in the training of military specialists (Tactical level of Military Education) according to the compatible NATO Standards." *Bulletin of Science and Education* 11 (17). https://doi.org/10.52058/2786-6165-2023-11(17)-770-784.

Marija, Doric, and Glisin Vanja. 2023. "The use of artificial intelligence in the Russo-Ukarinian war." *Politika nacionale bezbednosti* 25 (2): 59-76. https://doi.org/10.5937/pnb25-47369.

Mozur, Paul, and Adam Satariano. 2024. "Russia, in New Push, Increasingly Disrupts Ukraine's Starlink Service." *The New York Times.* https://www.nytimes.com/2024/05/24/technology/ukraine-russia-starlink.html.

NATO. 2023. *Electromagnetic warfare.* https://www.nato.int/cps/en/natohq/topics_80906.htm.

Sirenko, A.S. 2024. "The Role of Artificial Intelligence in Making Foreign Policy Decision in the Ukrainian- Russian War." *European Socio-Legal & Humanitarian Studies* (No.1): 122-128. https://doi.org/10.61345/2734-8873.2024.1.13.

Skove, Sam. 2024. *Another US precision-guided weapon falls prey to Russian electronic warfare, US says, Defence One.* https://www.defenseone.com/threats/2024/04/another-us-precision-guided-weapon-falls-prey-russian-electronic-warfare-us-says/396141/.

Spirin, Denis, Olecsandr Pogorilyi, and Olga Shynkarenko. 2023. "Justification of modernization paths for short-range air defense missile systems of land forces." *Scientific works
 Of State Scientific Research Institute of Armament and Military Equipment Testing and Certification* 16 (2): 75-81. https://doi.org/10.37701/dndivsovt.16.2023.11.

Spotlight, Japan. 2023. "The usages of Data from Space." *Special Interview.* https://www.jef.or.jp/journal/pdf/249th_Special_Interview.pdf.

Tenchi Sangyo Co., LTD. 2021. *Tenchi Sanhyo Packaging Machines.* https://www.tenchi.jp/en/aboutus/.

Tenchi. 2024. "Tenchi Security raises a $7 million Series A from Bradesco, L4 Venture Builder, and Accenture." *News.* https://www.tenchisecurity.com/en/insights-news/tenchi-security-raises-a-7-million-million-series-a-from-bradesco-l4-venture-builder-and-accenture.

Tokyo SME. 2023. *Leakage Risk Assessment & Management Software: Tenchijin CMPASS KnoWaterleak.* https://tokyo-smes.com/en/productservice/management-software/.

Topor, Sorin. 2024. "The importance of military sciences to ensure national survival in future conflicts ." *Journal: Annals – Series on Military Sciences* (No. 1). https://www.ceeol.com/search/article-detail?id=1248442 .

Tzu, Sun. 2026. *Arta războiului* . București: Editura Art.

Van Haaster, Jelle. 2019. "On Cyber: The utility of military cyber operations during conflict." *[Thesis, fully internal, Universiteit van Amsterdam], UvA-DARE (Digital Academic Repository).* p. 90. https://pure.uva.nl/ws/files/37093787/Thesis.pdf.

Willett, Marcus. 2022. "The Cyber Dimension of the Russia-Ukraine War." *Survival: Global Politics and Strategy* 64 (5): 7-26. doi:10.1080/00396338.2022.2126193.

Wright, Timoty. 2022. *Hypersonic Missile Proliferation: An Emerging European Problem?* EU Non-Proliferation and Disarmament Consortium, Non-Proliferation and Disarmament Papers, No.80. doi:doi.org/10.55163/qvhv3959.

Youvan, Douglas. 2024. *The Shadow War in Kursk: Assessing the Potential Role of CIA Covert Operations in the Ukrainian Incursion int Russian Territory.* doi:10.13140/RG.2.2.15318.46404.

Титаренко, Олександр, and Євген Власенко. 2024. "ПРОТИПОВІТРЯНА ОБОРОНА В РОСІЙСЬКО-УКРАЇНСЬКІЙ ВІЙНІ: УРОКИ ТА РЕКОМЕНДАЦІЇ" ("AIR DEFENSE IN THE RUSSIAN-UKRAINIAN WAR: LESSONS AND RECOMMENDATIONS")." *Повітряна міць України* 1 (6): 49–55. https://doi.org/10.33099/2786-7714-2024-1-6-49-55.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Information operations, rivalry projects in the information arena

Lect. Cristinel-Marius AMZA, Ph.D.*

*"Carol I" National Defense University, Bucharest, Romania
e-mail: amza.marius@unap.ro

Abstract

The organization and conduct of intelligence operations in the Intelligence Arena involves a real rivalry and confrontation among the Intelligence Services, conducted in order to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying on the one hand to thwart each other's efforts to know the other, and, on the other hand, to mislead, misinform, or deceive.

Keywords:
intelligence operations; ISR; counterintelligence; clandestine; confidential; secret.

Article info
Received: 2 October 2024; Revised: 1 November 2024; Accepted: 13 December 2024; Available online: 17 January 2025

Citation: Amza, C.M. 2024. "Information operations, rivalry projects in the information arena."
Bulletin of "Carol I" National Defence University, 13(4): 221-233. https://doi.org/10.53477/2284-9378-24-60

At this point, we can say that the vast majority of security or defense strategies developed by the vast majority of the world's states refer, particularly, to national interests, which determine their actions on the international stage, ensuring their survival.
Gathering information about adversaries has been and still is essential to developing these military strategies since the emergence of rivalries. Knowing your opponents' capabilities, order of battle, and intent can make the difference between victory and defeat. Whether through human sensors and interception of communications or by observation from a hilltop or, in the modern age, from the highest level of space, the ability to know what the adversary is doing is essential to understanding and ultimately to aiming for victory.

In the current security environment, the dependence of national power on intelligence is obvious and it requires specialized structures to be capable of supporting the foreign policy desired by strategic decision-makers. Dominant states create and configure their intelligence services to enhance their power in international relations and, from this perspective, they are essential "arenas for power relations" (Morgenthau 2007; Evans and Wilson 1992, 330).

Intelligence means understanding the security environment, actors (NATO AAP-6 2021) and forces that pose a threat to a state. Knowledge means supporting the political and military actors and it is a part of the decision-making process and the result of collecting, processing, exploiting, integrating, and interpreting available information about the current security environment and threat.

Intelligence has two broad objectives: the first is to reduce uncertainty by providing accurate, timely and relevant information, threat and environmental knowledge and the second is to protect the homeland and citizens by conducting counterintelligence activities and actions.
The interests and the divergences of geopolitics, geostrategy, economics, and ideology among state actors will never allow decision-makers at the strategic level to have a clear picture of the security environment; that is why intelligence deals with the greatest number of unknowns and has to provide answers in order to know their true intentions. Almost always there will be gaps in the information and knowledge provided and the degree of detail desired will be lacking because information cannot provide absolutely everything with certainty. It uses probabilities but it tries to reduce uncertainty by confronting the competitor by gathering relevant information, placing in the context to provide knowledge, and passing it on to form the complete picture and improve its understanding; therefore, the execution of intelligence and counterintelligence operations by the intelligence services is extremely relevant.

From the point of view of intelligence operations, the approach to the intelligence arena is that it can be divided into three broad categories. The first category refers to the collection of data and information for processing, transforming it into

intelligence, and disseminating it to decision-makers. The second category refers to those intelligence operations undertaken to influence the course of events, sometimes called clandestine or secret operations. Finally, the third category refers to counterintelligence operations that are executed to counter-intelligence operations, regardless of who the rival is. All those types of intelligence operations will have an impact on any state's foreign policy. This impact will vary in both scope and degree of involvement because it is the political factor that approves the planning and execution of intelligence operations (Westwood 1977, 86).

An intelligence operation is a unique and complex project that is planned and executed over a medium to a long period of time, with experienced human resources and a huge consumption of material and financial resources to accomplish the objectives. Such a project consists of a varying number of phases, subphases, tasks, and collective and individual actions executed in a unified concept and the execution is possible only through the coordination and interrelation by a multidisciplinary group of intelligence personnel (collectors, analysts, technical, IT, etc.) of the phases, activities and tasks. The main objective of implementing the operation's project is to ensure the required performance and quality with the lowest achievement risk and in the most reasonable time.

Intelligence operations for the collection of data and information for processing and transforming it into finished intelligence products are necessary for military actions because they clarify the strategic, operational, and tactical environment, clarify the adversary's intentions, and are essential for the commander's decision-making. Intelligence encompasses the organizations, capabilities, and processes used to task, collect, process, analyze, and exploit information from multiple sources, with an ongoing focus on satisfying intelligence requirements of the joint force commander's (JFC), and intelligence operations are conducted in and from all domains throughout the competition (U.S. Air Force Doctrine 2023).
Intelligence enables leaders at all levels to make decisions based on intelligence to apply combat power. Success in operations requires timely and effective decisions based on the application of judgment and available knowledge. As such, commanders and staff seek to build and maintain ongoing situational understanding throughout the operation.

Intelligence operations encompass intelligence collection in all domains with the full spectrum of sensor capabilities, processing, exploitation, integrated analysis, and intelligence production activities at the large-unit level, operations centers (air, naval, and ground) distributed to beneficiaries, and national production centers. These operations produce and disseminate intelligence to tactical, operational, and strategic users through the intelligence cycle: planning and targeting; collection, processing, analysis, and production; dissemination; and evaluation and feedback. Importantly, evaluation and feedback are continuous and facilitated throughout the cycle through collaboration and dialogue with all stakeholders.

Joint Intelligence, Surveillance, and Reconnaissance (JISR) services are vital to all military operations and provide decision-makers and headquarters with better situational awareness of the operational environment. To enable the collection of information and to ensure that intelligence is analyzed and produced for decision-makers, there are several primary actors involved, including collection, surveillance, and reconnaissance assets (e.g. Alliance Ground Surveillance and Airborne Warning Aircraft & Control System, which uses radars, observation satellites, electronic assets, and reconnaissance structures to gather information), intelligence analysts and decision-makers.

Special reconnaissance is reconnaissance and surveillance conducted as a special operation in hostile, difficult-to-access, or politically and/or diplomatically sensitive environments to collect or verify information of strategic or operational importance, avoiding discovery and direct combat with the enemy. Special reconnaissance is carried out by small structures, such as a detachment or reconnaissance team, consisting of highly trained military personnel, usually from special forces units or military intelligence structures.

Special reconnaissance is different in purpose and its role, from commando actions, but both are usually carried out by the same type of structures. The special reconnaissance role includes direct support of air operations strikes by providing imagery, enabling aircrews to adjust flight strategy, as well as that of artillery and ground-based missile systems, in areas of operations deep within the enemy's air defense, the placement of remotely operated and monitored sensors, and specific preparations for the actions of other special forces or military intelligence structures. The myriads of missions that can be performed by special reconnaissance structures include direct actions on targets, as well as unconventional warfare, including guerrilla operations. In addition to being highly trained, special reconnaissance units are also equipped and weaponized with high-quality technology and weaponry, as they have to fight in difficult conditions, often with an unfavorable force ratio, when they are discovered and when the extraction elements are delayed in reaching them. During the first Gulf War in 1991, British SAS and US Air Force units were initially deployed deep into the Iraqi battlefield to find Scud Missile Launchers and direct air strikes. When air actions were delayed, the patrols attacked the critical infrastructure of the Scud systems with their weapons and equipment.

Following the execution of a special reconnaissance operation, structure debriefing might be done with HUMINT personnel who are most familiar with intelligence-gathering techniques. The information resulted is likely to contribute to the support of HUMINT intelligence collecting, but depending on the mission may also contribute to IMINT, SIGINT, MASINT, and TECHINT. Some of these techniques and procedures are highly sensitive and confidential and are managed on a "need to know" basis within the structures coordinating the special reconnaissance operation, including for members of the all-source intelligence cell.

Discreet, covert, or secret intelligence operations of a government, seeking to influence events in other countries, are only a small part of international relations, but they exist precisely to support decision-makers. Planning and execution of those types of operations have the distinct advantage of accomplishing policy without jeopardizing the national aspect, and regardless of their nature, when intelligence structures fail, they do not leave the bitter taste of defeat as in a confrontation.

The long-considered axiomatic doctrine that even if a state's involvement in a covert action becomes known, the head of state should be able to deny that he authorized or even had knowledge of it is closely related to the aforementioned. He should be able to state, quite plausibly, that the operation was carried out by his subordinates who acted without his knowledge or authorization (Shulski and Schmitt 2008, 151). Intelligence operations aimed at influencing events can be categorized into the following types of operations: "discreet", "undercover", "clandestine" and "false flag". In this article, I will use the term "discreet" operations to differentiate it from "covert" and "clandestine" operations.

A black operation is a covert operation by a government agency, a military entity, or a paramilitary organization and may include activities, including those of private entities, with the primary objective of clandestine or covert entry into a competitor's target structures to obtain information using human sources. This is obviously the best situation in the case of information gathering since access to secret documents or fragments of useful or necessary information is gained. The basic characteristics of a discrete operation are that it is confidential and cannot be attributed to the organization conducting it (Smith Jr. 2003). This type of intelligence operation has been planned and executed by most specialized services such as MI6, MI5, Mossad, CIA, KGB, FSB, and ISI, as well as intelligence structures of other states (Intelnews 2008).

The major difference between a discreet operation and a secret one is that a discreet operation involves a significant degree of deception to hide who is behind the operation or to make it appear that another agency or entity is involved. A well-known example dates back to May 2007, when ABC News and, later, The Daily Telegraph reported that US President George W. Bush had authorized the Central Intelligence Agency (CIA) to undertake "discreet operations" in Iran to promote regime change and sabotage the nuclear program. Subsequently, ABC News was criticized for reporting the discreet operation, with 2008 presidential candidate Mitt Romney saying he was "shocked to see the ABC News report on the discreet action in Iran", but ABC said the CIA and the George W. Bush knew of their plans to publish the information and raised no objections (Montopoli 2007). In June 2007, the CIA declassified some of the documents and made them public detailing illegal surveillance, assassination plots, kidnappings, and other "discreet" operations undertaken during the 1950s and 1970s because they offered insight over a very difficult period and showed a different profile of a different intelligence agency on how to go about accomplishing its tasks.

A clandestine operation is an intelligence or military operation conducted in such a way that actions and activities go undetected by the local population or by the adversary's intelligence and counterintelligence structures. Until the 1970s, clandestine operations were primarily political in nature, generally aimed at supporting groups or nations that another entity favored. Examples include US intelligence involvement with German and Japanese war criminals after World War II or the failed Bay of Pigs Invasion, in 1961. Today, those operations are part of the modus operandi of many intelligence structures around the world and are carried out in a variety of ways depending on the technology available.

Most clandestine operations involve information gathering, usually by both humans and sensors placed in strategic areas or camouflaged in important locations. The placement of underwater or land-based communications cables, cameras, microphones, traffic sensors, monitors such as sniffers, and similar systems requires that the mission remain undetected and undetected. Clandestine sensors may also be mounted on unmanned underwater vehicles, reconnaissance satellites, unmanned aerial vehicles (UAVs), or unmanned detectors, or manually placed by clandestine human sources.

The terms clandestine and hidden are not synonymous. As stated in the definition (which has been used by the United States and NATO since World War II), in a covert operation the identity of the sponsor is concealed, while in a clandestine operation, the operation itself is hidden. In other words, clandestine means "stealth procedure", where the operation is not intended to be discovered. The term "stealth" refers to both a broad set of tactics designed to provide and maintain the element of surprise and to reduce the enemy's resistance to information gathering. Hidden means "deniable" so that if the operation is discovered, it is not attributed to a group or entity. Some operations may have both clandestine and hidden aspects, such as the use of hidden sensors located at great distances or human observers who can direct artillery and ground-based missile strikes and air strikes. The attack is obvious, but the component that was used to locate the target may remain stealthy.

In World War II, targets identified and located by cryptanalysis of radio communications were only attacked if aerial reconnaissance of the areas was also carried out or, in the case of the downing of Admiral Isoroku Yamamoto's plane, an observation which was the responsibility of the Coastwatchers (Coast Watch Organization, Combined Field Intelligence Service were Allied military intelligence agents stationed on remote Pacific islands). During the Vietnam War, the drivers of the truck attacked on the Ho Chi Minh Trail were unaware of the capabilities of US-owned sensors such as the Black Crow airborne device that pinpointed their trucks' location by engine heat.

At this moment in the North Atlantic Area, there is a vast critical infrastructure of undersea communication cable networks between Europe and North America, and

sites such as TeleGeography have detailed maps of the layout of cables with civilian uses (power, internet, etc.), but there are also military systems that are not the subject of such postings, as they contain essential data for all forms of communication between Alliance members. Relatedly, electronic reconnaissance vessels of the Russian Navy (e.g. Yantar – officially classified as an auxiliary general oceanographic research vessel with underwater rescue capabilities, which is subordinate to a separate structure from the military navy of the Russian Ministry of Defense) sometimes operate covertly (deactivation of the satellite identification system), in the vicinity of vital submarine cables, raising concern among military and intelligence officials for possible interception of secret communications.

A covert operation is an operation carried out by military or police structures that involves an undercover agent or troops acting under a supposed cover to conceal the identity of the responsible party (Carson 2018). Under US law, the Central Intelligence Agency (CIA) is able to conduct covert operations. The legislative framework has defined covert action as special activities, both political and military, that the US government can legally deny (Daugherty 2004). The effect of this legislative framework is reflected in the special attention that the US Congress gives to the CIA compared to other intelligence structures.

According to a 2018 study by University of Chicago political scientist Austin Carson, covert operations can have the beneficial effect of preventing differences from escalating into conflict or war. He argues that keeping military operations secret can limit the dynamics of escalation, as well as insulate leaders from domestic pressures, while simultaneously allowing them to communicate to the adversary their interest in maintaining a limited war (Carson 2018, 45).

When these operations are carried out by police structures, the term "undercover" means to avoid detection by monitoring personnel with duties and especially to conceal one's own identity (or use an assumed identity) in order to gain the trust of the persons or organization, to learn or confirm confidential information or to gain the trust of data subjects in order to gather information or evidence. Undercover operations are traditionally carried out by law enforcement agencies, and those who perform such roles are commonly referred to as undercover agents.

The first actions were carried out in 1883 on the territory of Ireland, they were aimed at combating the bomb-planting actions that the Irish Republican Brotherhood had started a few years earlier, and the agents who acted were for the first time trained in counter-terrorism techniques and tactics. In 1906 a similar activity was carried out across the United States when the "Italian squads" were established to combat and intimidate the crime of aggressive elements in poor Italian neighborhoods.

There are two main issues that can affect undercover agents. The first is maintaining their identity, and the second is reintegrating back into their normal work after

accomplishing the operational objectives. Living a double life in a new environment presents many challenges, as undercover work is one of the most stressful jobs a special agent can undertake. The biggest cause of stress identified is the agent's separation from friends, family, and his normal environment. The lifestyle of undercover agents is very different from that of normal police officers and after the mission is over it is difficult to reintegrate into the everyday tasks. After such a free lifestyle, agents may have problems with subordination, and discipline or feel uncomfortable, may have strange sometimes even paranoid views about the world and life, and may be constantly on alert.
Throughout history, there have been many covert intelligence operations aimed at gaining information about potential adversaries as early, as peacetime. In this context, it can be said that such operations are part of the mode of action of the intelligence services for the purpose of early warning of the political-military leaders (Piroșcă 2020).

A false flag operation is an act committed to disguise the real source of responsibility and place the blame elsewhere. The term has been used to describe a trick in naval warfare whereby a ship flew the flag of a neutral or friendly country in order to hide its true identity. The tactic was originally used by pirates and corsairs to trick other ships into allowing them to approach them before attacking them. Later, it was considered an acceptable practice during naval warfare under international maritime laws, provided the attacking ship displayed its true flag once the attack had begun (Ruis and Nilsson 2022).

At present, the term also stands for the organization of attacks by some nations against themselves and makes them appear to be of enemy nations or terrorist groups targeting them, thus providing a pretext for internal repression or triggering military aggression. In-ground military action, such operations are generally considered acceptable under certain circumstances, such as deception of the enemy, provided that deception is not perfidious and that all deception is eliminated before opening fire on the enemy.

Intelligence operations of this kind were used as a pretext for starting wars. Thus, the Gleiwitz incident on the night of August 31, 1939, had Reinhard Heydrich as the protagonist by fabricating evidence of a Polish attack against Germany in order to mobilize German public opinion for war and to justify war with Poland. Alfred Naujocks was a key organizer of the operation on Heydrich's orders which resulted in the death of several victims in some Nazi concentration camps who were dressed as German soldiers and then shot by the Gestapo to make it appear that they had been shot by Polish soldiers. This, along with other false flag operations in Operation Himmler, would be used to mobilize the support of the German population for the start of World War II in Europe (Lightbody 2004). The operation was unsuccessful because it failed to convince international public opinion of German claims, and Britain and France declared war two days after Germany invaded Poland.

In February 2022, intelligence structures of some Western governments warned about the possibility that the Russian Federation might be conducting a false flag operation to make the case for an invasion of Ukraine. The run-up to the February 24 invasion revealed an intensified disinformation and misleading campaign by the Kremlin and the Russian media by promoting "false flags" almost hourly, purporting to show the attack on Russia by the Ukrainian armed forces, in an attempt to justify an invasion of Ukraine. Many of the videos posted on social media were for disinformation having poor and amateurish quality, the metadata did not match as it showed incorrect data, and the evidence and arguments presented by Bellingcat specialists and other independent journalists made it clear that the claimed attacks, explosions and evacuations in Donbas were staged by Russia.

Similarly, in naval warfare such deception is permissible, provided the false flag is lowered and the true flag raised before engaging in combat (Squires 2008). A notable example was the German cruiser (formerly merchant ship) Kormoran of World War II, which surprised and sank the Australian cruiser HMAS Sydney in 1941 while disguised in a Dutch merchant ship, causing the highest loss of life on an Australian warship. While Kormoran was fatally damaged during the battle and her crew captured, the result was a considerable morale victory for the Germans.
In espionage, the term "false flag" describes the recruitment of agents by intelligence officers posing as representatives of a cause to which potential agents are sympathetic, or even the agents' own government.

In order to ensure the success of a state's international relations and military operations, strategic decision-makers must also arrange for the necessary measures to be taken to deny the adversary the possibility of carrying out acts of terrorism, espionage, subversion, sabotage, organized crime or attacking own communications and IT networks. In order to achieve this, it is necessary to identify the vulnerabilities of one's own entities to the execution of the adversary's intelligence operations, and the results of the analysis will be forwarded to the counterintelligence structures.

Counterintelligence (CI) includes those activities that relate to identifying and countering the threat to security posed by hostile intelligence services or organizations by persons engaged in espionage, sabotage, subversion, or terrorism (NATO Standard AJP-2 2016; UK Ministry of Defence JP 2-00 2023), and the best defense against attacks by foreign actors on the national territory, against the citizens of the country or the infiltration of intelligence services are active and flexible measures, having the ability to quickly choose counterintelligence techniques, depending on the evolution of the situation against those hostile services regardless of their affiliation. This defense is usually referred to as counter-espionage, i.e. measures taken to detect enemy espionage or physical attacks against friendly intelligence services, to prevent damage and loss of information, and where possible to turn the attempt against its originator. Counter-espionage goes beyond being reactive and actively seeks to undermine the hostile intelligence service by recruiting

agents into the foreign service, by discrediting personnel actually loyal to their service, and by taking resources that would be useful to the hostile service. All of these actions apply to non-national threats as well as national organizations.

If the hostile action takes place in one's own country or a friendly or allied country with the cooperation of police structures, the hostile agents may be arrested or, if they are diplomats, declared persona non-grata. From an intelligence service perspective, exploiting the situation to the party's advantage is usually preferable to arrest or actions that could lead to the death of the threat. The intelligence priority sometimes conflicts with the instincts of one's law enforcement organizations, especially when the foreign threat combines foreign personnel with the country's citizens.
In some circumstances, arrest can be a first step where the detainee is given the choice to cooperate or face serious consequences up to and including the death penalty for espionage. Cooperation may consist of telling all that is known about the other service, but preferably actively assisting in deceptive actions against the hostile service.

The protection of intelligence services is achieved by organizing defensive counterintelligence and involves assessing the risks to their culture, sources, methods, and resources. Risk management must constantly reflect those assessments because effective intelligence operations are often risk-takers. Even when taking calculated risks, services need to mitigate the risk with appropriate countermeasures, especially to discover the specific methods of the art of information sharing. Today's intelligence services are developing capabilities to explore other intelligence entities believed to be open and be able to undermine individuals within the intelligence community. Offensive counterintelligence is the most powerful tool for finding penetrators and neutralizing them, but it is not the only tool.

So, it is generally understood that governments engage in covert actions (as they engage in espionage), these are often illegal under the laws of the state on whose territory they take place. They may also be contrary to international laws, which is underpinned by the principle of non-intervention in the internal affairs of sovereign states, although this principle has increasingly gained weight in international jurisprudence since the end of the Cold War (Shulski and Schmitt 2008).
Decision-makers need information that is not controlled or manipulated by hostile forces. Because every intelligence discipline is subject to manipulation by adversaries, the veracity of information and the credibility of all means of collection are essential. Consequently, each counterintelligence organization will validate the reliability of sources and methods that relate to the counterintelligence mission following common standards.

When a foreign threat combines foreign personnel with a country's citizens, we are dealing with intelligence operations called the "fifth column". In common parlance, the term refers to those who betray their homeland, acting from within, usually in favor of an enemy group or another nation. In fact, the Petit Robert dictionary

defines the phrase as "enemy's secret intelligence services in a territory", and the Larousse as "an element working in a territory for the benefit of the adversary (under this name were designated in 1940 the agents of the German secret services who they acted in France)". The term also applies to actions organized by military personnel. The activities of a fifth column can be overt or clandestine. All persons and material and financial means established in secret can be coordinated to directly support an attack from outside the country. Clandestine activities for a fifth column can be materialized through terrorism, espionage, sabotage and disinformation. These actions are carried out exclusively on the national territory or even within the combat device (during the established or decreed states of emergency) by the secret sympathizers of an outside force.

The term "fifth column" originated in Spain (originally quinta columna) during the run-up to the Spanish Civil War. Its first known appearance is in a secret telegram dated September 30, 1936, which was sent to Berlin by the German charge d'affaires in Alicante, Hans Hermann Völckers. In the telegram, he referred to an unidentified "alleged Franco statement" circulating (apparently in the Republican or Republican-held Levantine area). This "alleged statement" claimed that Franco claimed that four nationalist columns were approaching Madrid and a fifth column waiting to attack from within (the term first appears in a Spanish publication after which the following day, on 4 October 1936, is taken up in the French publication Le Journal (Le Journal 1936).

The first identified public use of the term is in the October 3, 1936 issue of the Madrid communist daily Mundo Obrero, and by mid-October, the media was already warning about the famous fifth column. By the late 1930s, as American involvement in the war in Europe became more likely, the term "fifth column" was commonly used to warn of potential rebellion and disloyalty within US borders. Fears of betrayal were heightened by the rapid fall of France in 1940, which some blamed on domestic weakness and a pro-German fifth column, and in the United Kingdom in a speech to the House of Commons, Winston Churchill assured MPs that he would act as a strong hand against the activities of the fifth column.

Conclusions

The instruments of national power consist of assemblages of sources of power that must constantly adapt to changes in the international security environment or even those in the domestic environment of a particular state. The informational instrument is also exercised through specialized institutions and is designed to provide the leadership of states, and other institutions that are responsible for other instruments of power, with the data necessary to make the most appropriate decision. Like the diplomatic instrument, the information instrument is used both in times of peace and in crisis or war.

In this respect, intelligence operations are seen by the Intelligence Services as methods and means of using agents, infiltrating agents into foreign environments of interest, incursions into enemy territory, as well as actions to prevent acts of sabotage or terrorism on its own territory.
Intelligence is vulnerable not only to external threats but also to internal ones. Subversion, betrayal, and leaks expose vulnerabilities, government and military secrets, intelligence sources, and methods. The insider threat is a source of tremendous damage to national security, especially when agents have access to information about major, discrete, covert, or clandestine activities.

To plan, organize, and conduct intelligence operations, intelligence structures must continuously adapt their activities to the requirements of their commanders and the harsh and often changing conditions of the intelligence arena. This particularly involves mental and organizational agility underpinned by resilience, adaptation, and flexibility. It is normal for success to come later and therefore requires perseverance in actions, adapting quickly, and seizing opportunities as they arise. For each intelligence operation, an agency must develop a project-specific methodology, thus ensuring the uniqueness and complex nature of the activities, in order to successfully fulfill the intended purpose. The rapid adaptation of intelligence working methods to the operational environment obliges secret agents to improve the efficiency of intelligence gathering and the flexibility of working procedures, in order to cope with changing circumstances and to avoid the idea that there is only one way of working.

At this point, we can say that intelligence operations are a common action that is part of the tactics, techniques, and procedures of action of the intelligence services around the world, for the purpose of permanent knowledge of the intentions of the competitors or to the states in which hostility is manifested towards the state initiating such an operation, as well as for the support of military actions and early warning of political and military leaders at the strategic level.

In conclusion, the organization and conduct of intelligence operations in the "Intelligence Arena" involves a real rivalry and confrontation between the intelligence services, conducted to gain some advantages at the expense of others. Nothing is surprising in the fact that these rivals are constantly trying, on the one hand, to thwart each other's efforts to know the other and, on the other hand, to mislead, misinform, or deceive one another.

References

Carson, Austin. 2018. *Secret Wars: Covert Conflict in International Politics.* Princeton University Press.

Daugherty, William J. 2004. *Executive Secrets: Covert Action and the Presidency.* University of Kentucky Press.

Evans, Tony, and Peter H. Wilson. 1992. "Regime Theory and the English School of International Relations: A Comparison." *Millennium - Journal of International Studies* 21: 329 - 351.

Intelnews. 2008. *Tallinn government surveillance cameras reveal black bag operation.* https://intelnews.org/2008/12/16/04-11/.

Le Journal. 1936. "La Passionaria preche la terreur."

Lightbody, Bradley. 2004. *The Second World War: Ambitions to Nemesis.* Routledge.

Montopoli, Brian. 2007. *Știri CBS.* http://www.cbsnews.com/8301-500486_162-2842625-500486.html.

Morgenthau, Hans J. 2007. *Politica între națiuni, Lupta pentru putere și lupta pentru pace.* Iași: Editura Polirom.

NATO AAP-6. 2021. "NATO Glossary of Terms and Definitions ."

NATO Standard AJP-2. 2016. "Allied Joint Doctrine for Intelligence, Counterintelligence and Security." Edition A Version 2. https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP2.pdf.

Piroșcă, Valerică. 2020. "Operații de intelligence." *Colocviu Strategic* 6 (173): 2-3. https://cssas.unap.ro/ro/pdf_publicatii/cs06-20.pdf.

Ruis, Carlos Diaz, and Tomas Nilsson. 2022. "Disinformation and Echo Chambers: How Disinformation Circulates in Social Media Through Identity-Driven Controversies." *Journal of Public Policy & Marketing* (no. 42): 18-35.

Shulski, Abram N., and Gary J. Schmitt. 2008. *Războiul tăcut.* București: Editura Polirom.

Smith Jr., W. Thomas. 2003. *Encyclopedia of the Central Intelligence Agency.* New York: Facts on File Inc.

Squires, Nick. 2008. *HMAS Sydney found off Australia's west coast.* https://www.telegraph.co.uk/news/worldnews/australiaandthepacific/australia/1581972/HMAS-Sydney-found-off-Australias-west-coast.html.

U.S. Air Force Doctrine. 2023. "Air Force Doctrine Publication 2-0 - Intelligence." https://www.doctrine.af.mil/Doctrine-Publications/AFDP-2-0-Intelligence/.

UK Ministry of Defence JP 2-00. 2023. "Joint Doctrine Publication. Intelligence, Counter-intelligence and Security Support to Joint Operations." https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.

Westwood, James T. 1977. "A contemporary political dilemma: the impact of intelligence operations on foreign policy." *Naval War College Review* 29 (4): 86-92. https://www.jstor.org/stable/44641751.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Exploring competitive intelligence in Romania: understanding corporate views and approaches

Adina MIHĂESCU, Ph.D.*
Lect. Raluca LUȚAI, Ph.D.**

*Babeș-Bolyai University, Department of International Studies and Contemporary History – Faculty of History and Philosophy
e-mail: adina.mihaescu@ubbcluj.ro
*Babeș-Bolyai University, Department of International Studies and Contemporary History – Faculty of History and Philosophy
e-mail: raluca.lutai@ubbcluj.ro

Abstract

The awareness and application of Competitive Intelligence (CI) in Romania are significantly less developed than in international markets. This disparity is evident in the limited understanding of CI methodologies and the insufficient allocation of resources dedicated to fostering a CI-oriented culture within Romanian enterprises. Furthermore, the perspectives of market participants on the importance and use of CI have not been thoroughly examined, highlighting a considerable gap in systematic research on this topic.

This study aims to address this gap in the existing literature by exploring the perceptions of Romanian firms regarding CI-related activities. Employing a qualitative methodology, the research seeks to assess how organizations recognize the benefits of CI, the extent to which these practices are integrated into their decision-making frameworks, and the obstacles that hinder their implementation. By doing so, this study enhances the understanding of CI within the Romanian context and establishes a foundational framework for promoting and advancing CI practices in the local economic landscape.

Keywords:
competitive intelligence; Romania; companies; perception.

Article info
Received: 15 October 2024; Revised: 8 November 2024; Accepted: 6 December 2024; Available online: 17 January 2025

Citation: Mihăescu, A. 2024. "Exploring competitive intelligence in Romania: understanding corporate views and approaches". *Bulletin of "Carol I" National Defence University*, 13(4): 234-248. https://doi.org/10.53477/2284-9378-24-61

Competitive intelligence - conceptualization

While for intelligence services, information is the key to national security, helping them to perform or maintain a level of security, for private companies - whatever their sector - information means profit and success against competitors. Competitiveness is making firms increasingly preoccupied with collecting and using information, and the process itself is becoming more sophisticated. Societies have a pressing need not only to possess information but above all to select it and transform it into knowledge to support decision-making. "Knowing the right things at the right time and acting on them is essential to achieving success." (Cook and Cook 2000) The focus therefore falls not only on raw information, but it is also relevant from the perspective of usefulness, with the timing of obtaining it being as important as the information itself. It is in this context that a particularly important concept for business - competitive intelligence - is emerging and developing.

Competitive intelligence (CI) is defined as any combination of data, information, and knowledge concerning the business environment in which a company operates that, when processed, provides a significant competitive advantage or enables informed decisions to be made based on sound analysis of all relevant factors and available options (Larry 1996, 16). Another definition emphasizes that Competitive Intelligence is "the process by which companies inform themselves about all aspects of rivals' activity and performance. It is an essential element in which the planning, not only of marketing campaigns but also of competitors' production programs, human resources, financial and other activities, can be directly or indirectly influential" (Larry 1996)

This field is one that emerged as a result of the realization of needs or shortcomings in management activity, being scientifically and methodologically transposed into research later. It therefore does not emerge from academic reflections, but rather from observations and business needs. The role of economic intelligence is obviously important throughout history, but we can approach this component of the business environment from the second half of the 20th century. Some of the first scholarly works in this area appeared in the United States. One of the earliest works dealing comprehensively and systematically with the process of competitive intelligence appeared in the United States of America and belongs to Michael Porter. Published in 1980, the book *Competitive Strategy: Techniques for Analyzing Industries and Competitors* was addressed to economic actors and aimed to solve a problem identified in the way management decision-making takes place. The work also presents a number of general techniques for analyzing the competitive environment and proposes models for setting strategies (Porter 1980).

In today's world, anticipating the rapid changes and transformations occurring in markets or different industries is a challenge that company leaders are finding increasingly difficult to manage. Based on given situations, the formulation of

strategies (short-term, medium and long-term) is an important step on which the very survival of the company depends. CI analysis involves a vast process by which the identified information is sorted according to its usefulness, evaluated, analysed and finally entrusted to decision-makers in the form of a complex analysis aimed at gaining a competitive advantage. The essential goal of every manager is to make a profit (or as much profit as possible), and this is one of the main economic indicators of whether the chosen strategies are favourable. It is important to emphasize here that the impact of a CI analysis is not immediate and cannot be immediately seen in the increase in the company's profit. From the perspective of improving product quality, CI processes bring a multitude of benefits through the innovation they bring to companies as well as to the sectors and areas in which they operate. Competitive intelligence involves two lines of work: one inward (the internal environment of the company) and one outward. While the former is aimed at an in-depth analysis of each individual department, with work structures, processes and organizational charts, the latter is aimed at a fundamental knowledge of the competition (Cook and Cook 2000).

All companies, regardless of their size, need Competitive Intelligence. As long as the concept of competition exists, competitive analysis is necessary. Technology and the ability of consumers to shop online is transforming competition, internationalizing it, irrespective of the size of the company. In order to stay in a market or to be successful, small businesses need to be aware of their competitors, identify their strengths and weaknesses, and what their existing or future strategies are.

In Romania, the level of knowledge and use of the concept of Competitive Intelligence (CI) is still underdeveloped compared to other international markets. The lack of consolidated knowledge and practices around CI, together with the limited resources allocated to this field, contribute to a low integration of intelligence practices in the strategies of local companies. At the same time, the perception of economic agents in the market towards the importance and usefulness of CI remains insufficiently known, as there are few studies or research that systematically explore how economic actors relate to this strategic process. Our study aims to fill this gap in the literature by initiating a structured analysis of the perceptions of Romanian companies regarding the use of specific Competitive Intelligence (CI) activities. Using a qualitative method, the research aims to explore to what extent the Romanian organizations are aware of the benefits of CI, how they integrate these practices in their decision-making processes and what barriers they perceive in their adoption. Thus, our approach contributes not only to a deeper understanding of the subject but also to the creation of a useful reference framework for the development and promotion of CI in the Romanian economic context.

In the following, we will outline the design of the research, as well as the main findings resulting from the interviews conducted with representatives of Romanian companies.

Research design

Based on the aforementioned assumptions, this paper uses the qualitative research method based on the semi-structured interview, a method that will help us to understand how Romanian companies relate to the practice of competitive intelligence.
The field of competitive intelligence combines elements from the fields of intelligence and economic studies. The point of congruence of the two fields is the uncertainty that can only be erased from the decision-making process by means of information.

Case selection
Our study aims at the perception of economic agents in Romania regarding the concept of competitive intelligence. We therefore propose an analysis of the Romanian economic environment, based on the perceptions of economic actors, their vision and their ways of resisting and developing. What is important for us is the attention these economic agents pay to the competitive environment and the strategies they use in this direction. In other words, we try to explore the causal mechanisms at work in a general relationship (Jason 2008). In this respect, we will use the single-case method, the case of Romania.
The Atlas of Economic Complexity, a tool for research and exploration of global trade flows in international markets, developed by the Harvard Kennedy School of Government following research conducted by the Harvard Growth Lab, ranks Romania 44th (out of 133) among the world's richest economies, with a 3.9% growth over the last five years. It is estimated that our country presents a dynamic and complex economic environment, with real possibilities for growth and development in the coming years, considering that the post-communist transition period from a centralized economy to a free trade economy is completed (Growth Lab n.d.). There are also a number of particularities of the Romanian economy which differentiate it from the other states of the European Union: the most interesting for our study is the fact that the level of competitiveness and performance indicators is below the European average (Valentin 2017). A democratic state for 34 years, a member of NATO for 19 years and a member of the European Union for 17 years, Romania is a young capitalist country. It is necessary to analyse the economic environment, through the prism of the actors/companies that operate within it, studying, interpreting and analysing their perceptions, the reasoning based on which they carry out their activity and also their own methods of interpreting the complexity of the economic environment within which they operate and develop.

Data collection method
In our opinion, a qualitative analysis of the business environment in Romania, from the point of view of information and competition, can be most comprehensively done with the semi-structured interview. The polyvalent nature of the relationship between the economy and intelligence is difficult to quantify through statistical methods, which motivated the choice of the interview. This facilitates a structured

dialogue with questions and answers aimed at revealing the companies' views on the field of competitive intelligence.

The semi-structured interview gives us flexibility and the possibility to adapt the questions according to the answers given by the interviewee. The interaction will be personalized, open-ended, and timely to explore a topic about which there is not much data available. This environment will give us much more insight into the perceptions of companies and allow us to explore topics that we had not initially considered.

From the perspective of the sample, since it is impossible to survey the entire population in an analysis, a representative sample is established, and interviewing them leads to results that can then be generalized (Kalika, Mouricou and Garreaun 2009). The selection of respondents was based on diversity, so the discussions were held with representatives of companies from vast areas and fields of activity, which are active (but not only) in the Romanian market. As the field of business intelligence is not easily accessible to all, large companies with a turnover (in the last three years) of more than one million lei were selected. Although the number of companies contacted for the interview was considerably higher, in the end, the number of responses was 23.

The discussions were conducted: face-to-face – with eight respondents (35%), via video computer applications - with eleven respondents (48%) and by telephone – with four respondents (17%). The period of the interviews was approximately 10 months, from August 2022 to May 2023, and the average duration of a meeting was 30 minutes. Out of the total of 23 respondents, 19 requested to sign a non-disclosure agreement (NDA) which required the interviewer to maintain the confidentiality of the discussion itself and the data and information provided. This was requested even though each respondent was assured of anonymity and GDPR (General Data Protection Regulation) regulations and that the purpose of this research was purely academic and scientific.

In terms of content, the interview grid consists of three parts: the first part, in which data about the company in question are obtained, the level of understanding of the subject of CI, perceptions on the importance of information in the business environment; the second part – to which those who state that they undertake CI actions respond; and the third part – to which those who state that they do not undertake CI actions respond.

Respondents' profile

The respondents in our study represent people from the management of companies that were chosen based on several criteria. Thus, the following criteria were used in the selection of respondents: turnover, number of employees and company affiliation (Romanian company/multinational company). Turnover is relevant, first of all, as it indicates the total sales, and the total business operations, in fact, realized by a company in a given period (usually one year). It highlights the very conduct of a company's business, establishing the total sales (and total revenues) made. Going further, according to Law 346 of July 14, 2004, on stimulating the creation and

development of small and medium-sized enterprises, turnover classifies companies into (a) small and medium-sized enterprises (number of employees less than 250 and net turnover up to €50 million) which in turn are divided into -micro-enterprises (up to 9 employees and turnover up to €2 million), - small enterprises (10 to 49 employees and turnover up to €10 million) and medium-sized enterprises (50 to 249 employees and turnover up to €50 million). The second broad category is large companies and corporations (more than 250 employees and turnover of over €50 million). Based on these legislative elements, the profile of respondents is as follows:

TABLE NO. 1

Classification of respondents

Company type	Number of respondents
Corporations	5
Medium-sized enterprises	8
Small enterprises	8
Micro-enterprises	2

An overview of respondents can be found in the box below:

TABLE NO. 2

Respondents' profile

Assigned code	NACE Code*	Turnover**	Number of employees***	Multinational company	Romanian company
C 1	6419 – Other monetary intermediations	6 billion lei	5,000	Yes	
C 2	4646 – Wholesale of pharmaceutical goods	3 billion lei	700	Yes	
C 3	4120 – Construction of residential and non-residential buildings	20 million lei	45		Yes
C 4	4120 – Construction of residential and non-residential buildings	20 million lei	20		Yes
C 5	7311 – Advertising agencies	90 million lei	40	Yes	
C 6	7022 – Business and other management consultancy activities	2.5 million lei	10		Yes
C 7	7022 – Business and other management consultancy activities	1 million lei	5		Yes
C 8	4520 – Maintenance and repair of motor vehicles	50 million lei	50		Yes
C 9	6201 – Computer programming activities	200 million lei	600	Yes	
C 10	6201 – Computer programming activities	180 million lei	600	Yes	
C 11	6201 – Computer programming activities	170 million lei	500	Yes	
C 12	9200 – Gambling and betting activities	90 million lei	50		Yes
C 13	4711 – Retail sale in non-specialised stores with food, beverages or tobacco predominating	130 million lei	200		Yes
C 14	4764 – Retail sale of sporting equipment in specialised stores	350 million lei	80	Yes	
C 15	4791 – Retail sale via mail order houses or Internet	25 million lei	15		Yes
C 16	8559 – Other education n.e.c.	10 million lei	50		Yes
C 17	8559 – Other education n.e.c.	5 million lei	10		Yes
C 18	0150 – Mixed farming	180 million lei	120		Yes
C 19	0147 – Raising of poultry	150 million lei	600		Yes
C 20	0121 – Growing of grapes	150 million lei	100		Yes
C 21	6920 – Accounting, bookkeeping and auditing activities; tax consultancy	10 million lei	10		Yes
C 22	6492 – Other credit granting	33 million lei	100		Yes
C23	2351 – Manufacture of cement	2 billion lei	1,000	Yes	

Data analysis method

Our study uses inductive thematic analysis as a method of data analysis, which focuses on understanding and interpreting practices and experiences rather than measuring variables using mathematical processes. Based on the theoretical concepts studied, we considered that inductive thematic analysis harmonizes best with the study of the perception and understanding of Romanian companies in the field of Competitive Intelligence. Moreover, it allows an intrinsic approach to finding out the motivation behind the decision and the way companies choose to undertake CI actions. Thus, as a result of the interviews conducted, large recurring themes were identified, which we will discuss in the following section.

Analysis

This paper gives an epistemological approach to the field of Competitive Intelligence in Romania. Based on the research carried out, is it evident that the domain is insufficiently studied in our country, and what is more, it is insufficiently known and understood by the private sector.

Competitiveness is not exclusively a private sector concern but encompasses national and European policy interests. These structures are willing to pay increased attention and involvement in this direction, considering competitiveness a *sine qua non-principle* of sustainable economic development. According to the European Commission, competitiveness is particularly important "as it reflects the sustained increase in a nation's standard of living". (European Commission 2023). Mișu Negrițoiu, President of the Financial Supervisory Authority (ASF), stated at a conference of the NBR: "Competitiveness is created mainly at the microeconomic level; sustainable prosperity is created by firms in a favourable macroeconomic environment, and the factors that determine the level of productivity are: investment, the ability to innovate and competition." These three aspects mentioned are particularly important in a developed market economy; in our paper, we will address the third one through the prism of Competitive Intelligence.

Level of understanding of competitive intelligence

Literature offers a number of complex definitions and approaches to the CI domain, but this paper explores how the respondents, i.e., the companies interviewed, perceive it.

From the total of 23 interviewees, 8 (C3, C4, C8, C12, C13, C15, C16, C22), (34.8%), state that they have never heard, therefore not knowing the concept of IC, resulting in 65.2% of those who have encountered this concept during their work. During the discussions, those who say that they are not familiar with the concept try to clarify themselves, to get more details or even try, in the form of questions, to clarify the concept: "Does it refer to espionage?" or "Is it a new field brought in by some foreign business?". On the other side, there is the category of respondents who say that they have encountered the concept in the course of their work. Those who can define it

capture the following aspects, which are also correct: analysing information about competitors, collecting and analysing existing data on the market, protecting their own sensitive data, and improving performance: "Competitive Intelligence (CI) is the process of collecting and using relevant information about competitors – customers, suppliers. It helps us better understand the business environment" (C2).
In category number three, there are those respondents who state that they are familiar with the concept of CI but when asked to define it do so incorrectly. A frequently encountered element is that competitive intelligence is still confused with espionage and intelligence service activity: 'It has to do with intelligence services and companies spying on each other' (C20). This is due to the suspicion surrounding the intelligence field in Romania. Communication of intelligence institutions with the public has failed to clarify the difference between espionage (e.g., industrial) and competitive intelligence which remains a poorly addressed area.

We tried to find out whether respondents have any knowledge about companies using CI, in Romania or abroad, and which exactly they are. 12 respondents said that they were aware of such companies, but were not certain, which is why we were not given the names of any such companies. Similarly, in trying to find out whether respondents were aware of companies in their field of activity that use CI, we received 7 affirmative answers. Asked further if they could tell us which they were, they chose to answer vaguely. Interestingly, this category of respondents is also aware of training courses in this field and of companies that offer CI consultancy. We noticed that all the mentioned consultancy companies are from outside Romania, and none of them are local. Respondents mentioned the lack of Romanian companies in this field and attributed it to the insufficient development of it in our country. In addition, some of them even mentioned the fact that there is no culture in this field.

Perceived importance of information

Not surprisingly, the saying "information is power" seems to be internalized by all respondents to our interview. Asked about the importance they attach to information, the respondents unanimously replied that they consider themselves to be up to date with market dynamics and the competitive environment in which they operate - "in our field of activity, anyone who is not up to date with the latest information, the latest technologies, will not survive in the market" (C4). The value they attach to the information they hold is also underlined by the fact that all respondents mention the importance they attach to data/information protection. Whatever the field of activity, they are all concerned that data about their companies, recipes, and patents should not be made public ("We have valuable production recipes that we protect, which are secret" (C7)). Also, in this category, the confusion between information obtained from open sources, in a legal way, and espionage is maintained. One respondent even tells us - "we don't deal with that [CI] because espionage is illegal and we don't want to get into trouble". In other words, as mentioned above, many interviewees associate connotations of espionage with this totally legal practice, confusing the two concepts, or failing to see any noticeable difference between them.

Companies undertaking competitive intelligence actions

One of the major themes we addressed, according to which we split the respondents and structured the interviews, is the one that results in two kinds of approaches: companies that undertake and companies that do not undertake CI activities.

In the first category, we find 7 companies out of the total of 23 interviewed (30.4%), namely: C1, C2, C5, C9, C10, C11, and C23. In the table below we can observe the profile of the respondents-companies carrying out CI activities.

TABLE NO. 3

Profile of companies carrying out CI activities

Company	Turnover (average)	Number of employees (average)	Company type
C1	6 billion lei	5,000	Large company/corporation
C2	3 billion lei	700	Large company/ corporation
C5	90 million lei	40	Medium-sized enterprise
C9	200 million lei	600	Medium-sized enterprise
C10	180 million lei	600	Large company/corporation
C11	170 million lei	500	Large company/corporation
C23	2 billion lei	1,000	Large company/corporation

As we can see, the profile of the companies undertaking CI actions is large companies, with a turnover of more than 18 million euros, most of them corporations (i.e., turnover of more than 50 million euros and more than 250 employees). In fact, out of the total of 7 companies, 5 are large companies/corporations and only 2 are medium-sized companies (turnover of more than 10 million euro and more than 50 employees). Of these, most have started their activities specific to the field of the study from the moment they started their activity in Romania. Of course, one of the reasons for this is that all of these companies have an old, tested organizational structure that did not have its roots in Romania.

A few of the companies (2) that have subsequently introduced the CI component into their business believe that there are noticeable differences in what it means to improve the company's business. This is reinforced by aspects related to (1) the importance of anticipating surprises - „we are much more aware of the reasons for the competition's decisions, they are no longer surprises", (2) the need to innovate - „we launched new products on the Romanian market, which did not exist before, by studying foreign companies" or (3) carrying out pragmatic, profitable activities - „because we understand the market better, we negotiate better with suppliers, obtaining advantages".

We were interested in finding out whether these companies have in-house CI departments/structures or if they outsource these activities. 5 (71.4%) of them have outsourced the CI area, in the sense that specialized companies in the field are in charge of it. No names of such companies were disclosed, 4 of the respondents only mentioning that they are not Romanian companies. One of the respondents stated that they have created their own CI department within the company, and another respondent stated that, although they currently have their own employees doing CI, at the beginning of the activity they collaborated with a specialized company from abroad (the motivation being a financial one).

Concerning the level of awareness of employees within the company about the CI efforts: all interviewees state that the vast majority of employees are not aware that the company where they work is engaged in CI activities. Only stakeholders, decision makers, top, and macro management are aware. As to the reason behind this decision, the answers are diverse, but have a common theme: „They don't need to know, we don't want it to be openly known in the market that we are doing this". On the one hand, companies want to protect their data, on the other hand, there is the fear of confusion that could arise among employees, most of whom are not aware of references in the field of business intelligence: („the data that we get through CI is very valuable, if this were found out it is possible that the process of obtaining it would be hindered, and in this sense, the large number of employees is a vulnerability" – C1).

As regards the usefulness of the information obtained with the help of the CI, all those with whom we spoke concluded that the data/reports obtained are particularly important. However, the way of working seems to be different for each company. Thus, we found the following situations: reports are requested whenever necessary (acquisitions, mergers, etc.) – C5, annual reports are received, containing analysis and forecasts for the following year/years – C2 or the CI department requests business meetings whenever they consider it necessary – C10. These reports and analyses seem to be useful in several situations listed by the respondents: profitability, sales growth, company credibility, cash flow, relationship with suppliers, rate of return on investment, company image, customer relations, market value, human resources, market share, turnover, adaptation/discovery of new technologies.

The discussions also led in the direction of analysing the future of the CI field in Romania, as it is seen by companies that are concerned with and concerned about this issue. We note that 71.4% of respondents believe that the CI field will develop in Romania. They attribute this to technological developments and the increasing openness of the Romanian market. Technologies such as AI (Artificial Intelligence) would bring new benefits in the field of business information but could also represent dangers for companies that do not understand, are not up to date with these technologies, or are unable to adapt. The development of the business consulting field in Romania could also bring about developments in CI activities.

Two respondents state that they do not foresee a development of the CI field in Romania. They put this down, on the one hand, to the financial resources needed by a company to undertake CI actions, which are more difficult for small companies to obtain. On the other hand, they consider that the (still) post-communist Romanian society is reluctant to easily accept terms such as intelligence, information, and counter-information, and tends to associate them with espionage and illegal actions. An education on the security culture would be necessary in this respect, all the more so as this area is not regulated by law in Romania.

Companies not undertaking competitive intelligence actions

The majority of the company representatives with whom we had dialogue stated that they do not undertake CI actions. The profile of the respondents who stated this can be analysed in Table 4.

TABLE NO. 4

Profile of companies not performing CI activities

Assigned code	Turnover (average)	Number of employees (average)	Company type
C 3	20 million lei	45	Small business
C 4	20 million lei	20	Small business
C 6	2.5 million lei	10	Microenterprise
C 7	1 million lei	5	Microenterprise
C 8	50 million lei	50	Small business
C 12	90 million lei	50	Medium-sized enterprise
C 13	130 million lei	200	Medium-sized enterprise
C 14	350 million lei	80	Medium-sized enterprise
C 15	25 million lei	15	Small business
C 16	10 million lei	50	Small business
C 17	5 million lei	10	Small business
C 18	180 million lei	120	Medium-sized enterprise
C 19	150 million lei	600	Medium-sized enterprise
C 20	150 million lei	100	Medium-sized enterprise
C 21	10 million lei	10	Small business
C 22	33 million lei	100	Small business

Out of a total of 16 interviewees who stated that they do not carry out CI actions, 2 (12.5%) are micro-enterprises, 8 (50%) are small enterprises and 6 (37.5%) are medium-sized enterprises. Their turnover is in the range of 1 million euro - 120 million euro and their number of employees is between 5 and 600. We note that there are no corporations in this category, as all those who agreed to be interviewed stated that they carry out CI operations.

The discussions held with representatives of these companies were different from those held with representatives of companies claiming to carry out CI activities, seeking to elicit the motivations and rationale behind the decision.

First of all, out of all the respondents (16) who stated that the companies they represent do not initiate CI actions, 37.5% justify the decision on the grounds of high costs („we are a small company, we cannot afford to invest in such a thing for the time being" – C6). However, only 3 respondents state that they are aware of companies that offer specialized courses and are aware of or have received pricing offers; the other 3 say that they are not aware of the prices charged by consulting or training firms in this field, they only assume that the prices charged would be high („I have never asked how much it costs because our budget does not allow us to offer courses or to hire more staff at the moment" – C20). This is important because it reveals that an important decision such as this one is based on assumptions, without any verification.

Another argument is of a moral, ethical nature. These refer, in fact, to the confusion made between CI (and business intelligence) and espionage. By equating the two

terms, even confusing them, the respondents state that the ethical values implemented in their companies do not allow them to deal with such actions („espionage is illegal, such practices would discredit us" – C12) and therefore are irrelevant for them („our company puts a very high emphasis on moral and ethical values, and we do not concern ourselves with approaches that do not fit into these values" – C18). Moreover, they even state that they would not trust companies that would carry out CI practices, but at the same time claim that they do not know such companies.

A recurrent motivation found during the discussions is based on a lack of knowledge of the CI domain. Thus, they do not start CI operations because they do not understand what it entails („I don't know how we could find out details about the competition, where we would find this information" – C15), who and what they should do in the company („the marketing department studies the competition and finds out what they promote" – C4). In this sense. 31.25% of those asked, do not deal with the field of business intelligence, or with the field of studying the competition because they do not know details about how they should do this.

For many respondents, one explanation for the lack of activity in this area is the lack of human resources. They claim that it would be useful for their companies to have some people/employees dealing with CI, but they do not know how and where they could find qualified staff. They consider that this area would not lend itself to being outsourced to a third-party company, but should be tackled by their own employees with skills in the field. There is support for the idea that if there was a ‚school' in this sector, producing accredited specialists, then it would be easier for companies to work in this area. Also, respondents do not see the usefulness of courses in the field for their own employees to do but would need "professionals" ("I don't trust fast-track professional qualification courses, especially in such a complex field." – C3); companies would find it easier to hire professionals in the field than to train their own specialists. In other words, these respondents do not consider an investment in training/retraining courses useful, preferring to hire professionals for each department/position and see specialization courses rather as bonuses that could be offered to employees. On the other hand, they do not object if employees want to take these courses and pay for them themselves.

Research limitations

The research that we have carried out has been challenging in many ways and this has an effect on the research findings. Based on interpretations from the data obtained, the research focuses on establishing perceptions, opinions or motivations present behind certain actions, and analysing decisions in depth. It establishes the relationship of economic agents to the field of Competitive Intelligence, their own visions and perceptions of the phenomenon; however, it is not without limitations. The aim was, more than obtaining some information, to understand the motivations

behind some behaviours, attitudes and phenomena in the Romanian business environment.
One of the limitations of the research is due to non-probability sampling, which makes it difficult to generalize the findings of the study to the whole country. On the other hand, the task of finding companies willing to provide information was difficult. Their reluctance can be justified by the fact that in a competitive environment, companies tend to protect their data from being made public and not to be known by competitors.

The interview can go into the depth of a complex topic, but subjects may be unwittingly influenced by the interviewer (even if the interviewer is neutral) or may give distorted information. Their behaviour may be dissimulative, and the interviewer may not notice this, which can make the information pervasive, distorted, or incomplete. During the interviews, we paid particular attention to these aspects but the limitation here exists. Another limitation is represented by the novelty of the field of Competitive Intelligence in Romania. On the one hand, this aspect creates confusion among companies about CI, as it is little known and understood.
As this is a sensitive issue for the subjects and the companies they represent, confidentiality and the protection of their identity are particularly important, both ethically and legally. Ensuring anonymity and confidentiality is a difficult issue to coordinate.

Conclusions

Our survey reveals that all respondents believe that information is important in business, although not all are actively and systematically concerned with obtaining it. Similarly, they all consider it important to study competition, although they choose not to do so, or not in a systematic and scientific way. The companies we spoke to know little about training opportunities in this area or about companies that can advise them.

An important recurring issue in the course of this research is the confusion between CI and espionage. On the one hand, this can be understandable, as there is not a sufficiently developed business intelligence culture in our country, the capitalist economy here being still quite new. On the other hand, the term intelligence, which is specific to the intelligence services, may be more difficult to transpose into the private sector in such a way that its meaning changes. Clearly, the CI works with open sources, but even this concept can pose problems of understanding for a layman/non-specialist. The association with espionage is also found among some who claim to know or have encountered the concept of CI, which shows that it is easy to be confused or that those who use it are not specialists or have not been informed by specialized, credible sources. In this paper, we have addressed a detailed

explanation of the differences between these two concepts, and we believe that it is useful to promote CI by mentioning precisely those aspects that distinguish and separate it from espionage.

Out of the total number of respondents, seven stated that they carry out CI activities (about 30%), and their profiles are of large, multinational companies. They claim that they have been carrying out IC operations since they first entered the Romanian market, which leads us to the conclusion that this practice is common and that multinational companies are aware of and use this area. This creates a disadvantage for Romanian companies which, for the most part, do not undertake such actions, do not attach so much importance to the competitive environment or, even more, are not aware that other firms do so. Thus, a large company knows in detail a market or the competition existing there, while a small company does not benefit from this advantage.

Those who undertake CI actions are fully satisfied and can state the benefits they bring to their companies. However, they prefer to keep this information hidden, not only from the public eye but also from their own employees. In terms of where CI activities take place, the vast majority of respondents use the services of external companies. We can deduce that these firms are not Romanian, due to the fact that the respondents, when asked, could only give examples of consultancy firms outside the country. Of those who have their own CI departments, one said that it is relatively newly built, as they were initially working with a consultancy firm. The difficulty in finding specialists in this field was again a recurring issue. There is a shortage of qualified personnel in the field of business intelligence in Romania, hence the preference to select foreign companies for collaboration from countries with a longer tradition in this field.

The micro and small companies interviewed state that they do not carry out CI actions, as do the vast majority of medium-sized companies. As mentioned above, we observe that this is rather a concern of large companies, which are also extended beyond the country's borders. The perception of smaller companies is that either CI requires the allocation of large sums of money or that it is not suitable for small companies and therefore would not be useful enough to justify the financial effort.

Although this significant allocation of money is discussed, it is rather a supposition, because the interviewees do not know the details of how much a course, expertise or collaboration with specialized companies would cost. Being a less well-known, rather new field, there is an assumption that expertise or consultancy would entail high costs. However, as companies are not aware of these costs, it is not possible to assess whether the benefits would outweigh them or what the cost/benefit ratio would be.

However, the vast majority of company representatives who say they do not carry out CI activities do not rule out this possibility. They are either open to this way of working, saying that they might do so in the future, or they are still sceptical about

the ability to allocate budget funds in this direction. The level of scepticism is high, mainly because the perception is that financial needs would be increased.

References

Cook, Michelle, and Cook Curtis. 2000. *Competitive Intelligence. Create an intelligence organization and compete to win.* Kogan Page.

European Commission. 2023. *Glosar de Politică Regională.* https://ec.europa.eu/regional_policy/whats-new/newsroom/27-03-2023-how-competitive-is-your-region-commission-publishes-the-regional-competitiveness-index_ro.

Growth Lab. n.d. *The atlas of economic complexity.* Accessed November 15, 2024. https://atlas.hks.harvard.edu/.

Jason, Seawright. 2008. "Case selection techniques in case study research: a menu for qualitative and quantitative options." *Political Science Research Quarterly* 294-305.

Kalika, Michel, Philippe Mouricou, and Lionel Garreaun. 2009. *La methodolie, le mémoire de master.* The free press.

Larry, Kahaner. 1996. *Competitive Intelligence. How to gather, analyze and use information to move your business to the top.* Simon&Schuster Inc.

Porter, Michael. 1980. *Competitive Strategy: Techniques for analyzing industries and competitors.* The Free Press.

Valentin, Vlad Ioan. 2017. *Strategia de dezvoltare a României în următorii 20 de ani.* Editura Academiei Române.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks

Dănuț MAFTEI, Ph.D.*
M.A. Student Lorin Nicolae BOGDAN-DUICĂ**

*National Cyber Security Directorate, Bucharest, Romania
e-mail: dn.maftei@gmail.com
**National Cyber Security Directorate, Bucharest, Romania
e-mail: bogdanduicalorin@yahoo.com

Abstract

Online social media platforms and search engines are used more and more by violent people, criminal offenders, cybercriminals, and other state or non-state malicious actors, who are involved in activities connected to hybrid threats and foreign interference, causing challenges for children, girls, women, citizens, societies, economies, critical services, democracy, and homeland security.

Social media platforms and search engines could do more to address these issues so as to ensure a free, open, safe, secure, and reliable internet for everybody and to maximize its positive effects. Neglecting the proliferation of illegal activities not only erodes trust in online platforms but also places at risk the security and privacy of its users.

To counter efficiently all the challenges, urgent new regulatory frameworks are needed. The regulations should be applied to social media platforms, search engines, and services that allow users to post content online or to interact with each other.

Keywords:

social media platforms; national security; democracy; malicious actors; foreign interference; false information; violence; frauds.

Article info

Received: 14 November 2024; Revised: 2 December 2024; Accepted: 6 December 2024; Available online: 17 January 2025

Citation: Maftei, D. and L.N. Bogdan-Duică. 2024. "Risks, threats, and vulnerabilities related to social media platforms and search engines. Regulations and national legal frameworks". *Bulletin of "Carol I" National Defence University*, 13(4): 249-265. https://doi.org/10.53477/2284-9378-24-62

The emergence of social media marked a new era for humankind, facilitating the evolution of humanity. Nowadays, there are several social media platforms (SMPs), search engines, and services that allow users to interact fast with each other or to post content online. This includes a variety of websites, apps, and other services, including social media services, video-sharing platforms, consumer file cloud storage and sharing sites, online forums, online instant messaging services, and dating services. They could be used for watching videos, gaining knowledge, sharing special moments, and reconnecting with friends.

On the other hand, these popular services and social media platforms also have a dark side because they can be a hotbed for scams, fraud, violence, disinformation, and false information. Online platforms and new technologies have made it easier, cheaper, and quicker than ever before for both domestic and foreign malign state or non-state actors to put them into practice. Moreover, anonymity and the lack of control and effective content verification mechanisms facilitate the spread of these messages and the identification of attackers. In parallel, the frequency and complexity of Tactics, Techniques and Procedures (TTPs) used by malicious actors to exploit the weaknesses of platforms and users are unceasingly increasing.

Social media platforms enable the rapid and widespread dissemination of false information and other forms of foreign interference that threaten democratic principles and values. They could be used to plan and display violent acts or spread fake news and harmful messages. Because activities conducted on SMPs can undermine democracy, polarize opinion, incite violence, shake trust in institutions, fuel discrimination and marginalization, and erode social cohesion, the impact on society is profound and complex. For instance, even individuals who do not use social media for violent purposes find themselves caught up in violence due to algorithms that are set to promote this kind of content and encourage acts that lead to real-life violence.
Scams originating from fake ads posted on social media have also increased dramatically. Even legitimate ads are cloned and used for malicious purposes, and for the end users it is hard to know whether the ad is legitimate without clicking on it (Alexander 2024).

The number of social media account takeovers is on the rise and the content is not necessarily checked, the reason why no one can be certain about interacting with someone known. Users should approach all social media interactions, whether it is a tweet, a post, or a direct message, with an appropriate dose of skepticism, being hard to recognize the signs an app cannot be trusted. For instance, since **online scams** (Stathis 2024a) and **Facebook Marketplace scams** (Alexander 2024) are so prevalent, it would be wise for users to learn how to identify a scammer (Stathis 2024b).

Malicious actors, especially the state ones, exploit social media platforms as means for conducting hybrid warfare operations. Researchers have especially noted the

evolution of Russian information warfare doctrine, along with its "deep roots in long-standing Soviet practice" (Giles 2016; Snegovaya 2015). The recent Russian military thinking emphasizes hybrid warfare as a new persistent reality, with the "information sphere" and "information warfare" as a critical battlespace.

So-called "trolls" and "bots" seem to play a key role in spreading **fake news** and **disinformation** through social media platforms. Professional trolls manage human-run accounts to provoke or spread disinformation and fake news on social media. On the other hand, bots are involved in managing automated accounts that combine human-generated content with computerized posting. To achieve their objectives, large networks of false accounts are created and used, which is why they play a significant role in promoting fake news.

Methods used by the social media companies to identify automated accounts and coordinated fake news campaigns conducted by state actors are different and the results are also diverse. Although platforms have implemented some content moderation measures, they are often insufficient and slow to respond the requests to remove harmful content. This is partly due to both the large volume of user-generated content and a lack of enough incentives to act quickly and efficiently. Despite its immense resources and technological prowess, *Meta for Business* has been criticized for its inadequate response to the proliferation of phishing scam pages on Facebook. The company's algorithms and content moderation mechanisms are often found lacking in means of identifying and removing these deceptive pages promptly, repeatedly replying to the request of the users that the "*content doesn't go against the community standards*", or that "*it is safe*". This leaves millions of users exposed to the risks associated with phishing scams, and it raises significant questions about Meta's commitment to user safety (Qureshi 2023).

Negative effects of malicious messages posted on social media platforms

The current scientific research has shown that malicious messages of various types that are posted on social media platforms have a negative impact both on individual users and on national security, democracy, and societal stability.
Foreign actors intend to create the conditions for manipulation or other interference by eroding public trust, destabilizing political systems, undermining democratic norms, and weakening the resilience of democratic states. In the long term, this can damage the ability of democracies to withstand external threats or maintain effective governance.

One of the most damaging effects of Foreign Information Manipulation and Interference (FIMI) is the erosion of public trust in democratic institutions. Misinformation, fake news, and hate speech, including targeting ethnic, religious,

and sexual minorities, amplify social divisions, lead to increased discrimination and violence against them, and fuel political and cultural polarization.
At the same time, trust in institutions and traditional media is eroded, leading to increased skepticism and difficulties in distinguishing between real and false information.

By exacerbating existing divisions in society, FIMI campaigns amplify the polarization of political discourse, making it more difficult for democratic societies to engage in constructive debate or identify common ground on the critical issues facing them. This polarization weakens the ability of democratic institutions to function effectively, turning the legislative process into partisan gridlock and political extremism.

SMPs, disinformation, hate speech, fake news, and cyber-attacks used to manipulate voters' opinions, as well as to increase social tensions and the level of violence before, during, and after elections, can influence the outcome of elections. Such activities can have far-reaching consequences as they can lead to the election of candidates who are more favorable to foreign interests or, conversely, harm the prospects of candidates perceived as hostile to such interests.
Women and teenage girls fall prey to various forms of online sexual violence (cyberbullying, rape videos, threats, and distribution of sexual images without consent). These forms of violence can become real and interfere with women's ability to feel safe at work or in public.

On the other hand, the popularity and ease of use of SMPs have made it easier for extremists to access like-minded people, create terrorist networks, recruit new members, spread extremist ideologies, and incite violence. SMPs algorithms can amplify extremist content, exposing users to dangerous messages that contribute to their radicalization. Foreign interference through health-related misinformation (e.g., on vaccines, pandemics, etc.) harms public health, increasing the risk of illness and premature death.
At the same time, misinformation and fake news can negatively affect national and international economies by manipulating financial markets, causing financial damage, undermining business confidence, and spreading panic.
Particular challenges are also posed by human trafficking for labor and sex trafficking, with children and even adolescents and young adults being the most common victims.

Tactics, Techniques, and Procedures used online by malicious actors for conducting fraudulent activities

Day after day both old and new TTPs can be seen that are used by scammers to trick people. With more and more online frauds being carried out every day, each

new fraud is even more complex, cleverer, and less detectable than the last one (Stathis 2024a). Currently, SMPs users are victims of several types of threats, which are summarized below.

Social media phishing (Adrien 2023) means attacks conducted online. Their purpose is to steal personal data or gain control of social media accounts. Phishing is a form of cybercrime where malicious actors impersonate trustworthy entities often to lure users through fake promotions, fraudulent contests, or fabricated news stories, or to deceive people into clicking on malicious links or revealing sensitive information such as personal details, login credentials, credit card information, financial data, etc. Phishing activities are connected to cybercrime, and they currently represent one of the most common forms of social engineering, with more than three billion spam emails sent every day.

According to statistics, millions of Facebook business accounts worldwide are being targeted with phishing messages, with a success rate of nearly one in seventy victims infected (Petkauskas 2023). Fraudsters usually impersonate SMPs in phishing attacks designed to sneak malicious software (spyware or ransomware) onto personal computers, and steal login information and potentially other personal data (Rosenkrantz 2024).

Phishing remains popular, but we could notice currently new phishing techniques like *spear phishing, whaling, business email compromise, smishing, https phishing, clone phishing, pop-up phishing, angler phishing, evil twin phishing, search engine phishing, watering hole phishing, vishing,* etc. (Chin 2024). Moreover, cybercriminals use generative artificial intelligence tools to write their emails, which significantly improves their phishing success rates.
Hackers use a massive network of fake and compromised accounts to send out millions of Messenger platform phishing messages to target Facebook business accounts with password-stealing malware (Toulas 2023b). According to reports (Zaytsev 2023), researchers warn that roughly one out of seventy targeted accounts is ultimately compromised, translating to massive financial losses.

Fraudulent applications (Budgar 2024) can be advertisements for apps or features on SMPs that claim to allow users to check who has viewed their profile.
In the case of the **Facebook Marketplace scams**, it can be seen that a huge number of users buy and sell goods every day, but also that scammers use this online shopping platform to scam people and steal their money (Alexander 2024). Scammers may ask users to pay or discuss additional details by using third-party communication channels, while others might list fake rentals, gifts, or various products.
In **bank fraud**, many scammers offer **fake gifts** to get users to divulge various personal information (credit card, social security numbers, etc.) or to access links where they can download viruses on their personal computers (Bradford 2024).

In **spoofing attacks**, hackers can illegally access a person's account and then send fake messages or posts to their friends asking for money or gifts (Alexander 2023). The messages are designed to excite or panic the user and then get them to provide money without properly analyzing the situation. In addition to using a friend's profile to conduct a spoofing attack, scammers might impersonate famous people or organizations.

Sextortion is a social engineering scam where a victim (usually male) is befriended by a female scammer, convinced to send sexually explicit images or videos of themselves to the fake persona, who then threatens to release live the compromising material if the victim refuses to pay up (Schappert 2024).

Attackers may also use **"Secret Santa" schemes** where people send a $10 gift to one person and then receive one from three others. But there is no guarantee that the victim will get their money back in these Facebook scams, because if no one follows through on sending the gift, they may get nothing in return. Malicious actors could use the victim's home address to carry out *doxxing attacks*[1] (Alexander 2022), and sharing other personal information could reveal the answers to password security questions, leaving personal accounts vulnerable to hackers.

[1] *Doxxing* or *doxing* is the act of publicly providing personally identifiable information about individuals or organizations, usually online and without their consent, as a form of punishment or revenge.

Misinformation refers to **false information**, misleading, or taken out of context, disseminated by *a p*erson who *believes it is true*, without intention to cause harm. Misinformation has the power of "social proof" in persuading individuals to accept false information. People could accept faster news stories as true when they are disseminated by friends, acquaintances, and supposedly credible sources, and when these stories are more popular overall (Hindman 2018).

Disinformation (PakVoices 2023) refers to **false information** (or manipulated narrative or facts, propaganda), and the *propagator knows it is false*. It is a deliberate, intentional lie, intended to manipulate, cause damage, and guide people, organizations, and countries in the wrong direction, generating mistrust in the democratic state institutions, either for the purposes of causing harm, or for political, personal, or financial gain.
Disinformation has multiple stakeholders involved; it is coordinated and hard to track. It may include doctored videos, fake news articles, and artificially amplified social media posts. It often contains slander or hate speech against certain groups of people and is often polarizing, inciting anger and other strong emotions and it can lead people to promote extreme views, and conspiracy theories, without room for compromise.
New emerging technologies are increasingly used to discredit factual information. Artificial intelligence (AI) and generative AI may be used to spread false and misleading information, such as "*deepfake*".

Malinformation refers to *reality-based information* that is used to harm individuals, social groups, organizations, or nations (ITU 2021). Malinformation involves real, not false, facts. Personal data and leaked emails revealed through *doxxing* are examples of malinformation. Harassment, hate speech, and revenge porn also fall into this category.

Fake news is *purposefully crafted*, sensational, emotionally charged, misleading, or totally fabricated information that mimics the form of mainstream news (Saint Francis University 2023). They are used for the online distribution of false information disguised as legitimate news stories. Motivations behind fake news could be personal (to harm an individual/business reputation), financial (to attract internet traffic and/or advertising income), or political (to influence the public's viewpoint/ideology).

***

Of course, there are plenty of other variations of challenges that people can face on the SMPs, such as *malware attacks, spam messages, cloned accounts, fake medical fundraising, clickbait scams, fake coupon code scams, Facebook quiz scams, romance scams, job scams, fake fundraising, cyber stalking, internet banging, child sexual abuse, control or coercive behavior, extreme sexual violence, extreme pornography, sale of illegal drugs or weapons, sexual exploitation, fraud, racially or religiously aggravated public order offenses, illegal immigration and human trafficking, promoting or facilitating suicide, abuse of intimate images (revenge porn), terrorism*, etc.

It needs to be clearly understood by decision-makers that all these types of TTPs represent an enormous number of possible ways of action that can be successfully used by various malicious actors to conduct complex online attacks with serious results. Following detailed scans of victims to identify their specific vulnerabilities, the attacks will then be organized, tailored, and customized exactly to the specifics of each target, combined with other state-of-the-art methods and technologies, so that the chances of success are maximized. As such, under these conditions, states need to adapt quickly by amending the legal framework and developing effective working strategies to counter such complex challenges.

Specific measures taken by national authorities for combating the illegal activities conducted by using social media platforms

It could be noticed that the EU and different countries around the world have been paying attention for years to the malign activities conducted on SMPs and to their impact on national security, democracy, state institutions, critical infrastructure, society, businesses, and citizens. The current research has highlighted several measures taken by national authorities against challenges posed by malicious actors (state and non-state) using SMPs, as follows.

The TikTok platform:

Since 2020, the TikTok Platform has been blocked/restricted in countries such as Afghanistan, Armenia, Azerbaijan, Bangladesh, India, Iran, USA, the reasons behind these decisions being related to national security, high levels of terrorism, border conflicts, etc. (Gordon 2024).

Under the Digital Services Act[2], the European Commission opened proceedings against TikTok over the launch of *TikTok Lite* in France and Spain (European Commission 2024).

[2] The Digital Services Act Regulation mandates that digital platforms take greater responsibility for the content shared on their platforms. This legislation seeks to limit the spread of harmful disinformation while ensuring that freedom of speech is respected.

In 2023, TikTok was banned on devices owned by state institutions in Austria, Belgium, Canada, Estonia, France, USA, due to security and privacy risks, as well as alleged links between the Chinese Communist Party and the company, with TikTok accused of collecting and sharing personal data with Chinese intelligence services (Lakshmanan 2024).

In May 2023, in Romania, the National Cyber Security Directorate – DNSC (a specialized body of the central public administration, under the authority of the Government, responsible for ensuring the cyber security of national civilian cyberspace), issued a recommendation to national state institutions and public bodies not to download, install and use TikTok on their networks and information systems (DNSC 2023b).

Taiwan had banned TikTok from government devices in December 2022. The reason was connected to concerns of it being used by China to carry on ”cognitive warfare” against Taiwan.

The technical reports on TikTok show the presence of *a lot of cybersecurity risks and vulnerabilities related to installing and using this application* (**collecting personal data, used devices, operating system, IP, SSID Wi-Fi, Serial number, SIM ID, IMEI, SMS reading, MAC Address, GPS location, user accounts, clipboard access, history, useless Do Not Track setting, services/applications used, user personal profiling, sharing collected data to other ”partners”, remote control, etc**.) (Baiaș 2023).

Meanwhile, the Chinese legal framework, which obliges citizens and entities to cooperate with intelligence services and state institutions to provide data and information for “national purposes”, was taken into account (***The State Security Law*, 2015; *The Cybersecurity Law*, 2016; *The Law on State Intelligence Activities*, 2017; *The Law on State Counterintelligence Activities*, 2023**).

The Facebook platform:

Since 2015, Facebook has been blocked in Ethiopia, Bangladesh, Myanmar, and Sri Lanka to prevent the spread of disinformation and hate speech, control the flow of information, and suppress dissent, on national security grounds or because of content deemed offensive to Islam.

Facebook, on the other hand, has been subject to restrictions and censorship in China, Iran, and North Korea, where access to the platform is either completely blocked or severely restricted.

Instagram:
Instagram has been blocked in China since 2014 as part of the Chinese government's efforts to control the flow of information and limit access to Western social media platforms. Meanwhile, Instagram was blocked intermittently in Iran during political unrest and protests to prevent and stop the spreading of information and coordination of demonstrations.
Turkey temporarily blocked access to Instagram and other SMPs after an attempted coup to prevent the spread of misinformation and panic (2016).

In 2020, India banned Instagram and around sixty other Chinese apps, citing national security and data privacy concerns (2020). In the same year, the Russian Federation blocked Instagram as a response to Meta's decision to allow users in certain countries to post calls for violence against Russian soldiers in the context of the war in Ukraine.
Instagram has also been subject to restrictions and censorship in North Korea and Turkmenistan, where internet access is strongly controlled by the national government.

The current legal framework issued by EU/EU member states and non-EU countries for regulating social media platforms

The European Union and several countries around the world have been paying attention to legal and regulatory frameworks to make the use of internet services safer for citizens, organizations, and businesses, but also to make social platforms more accountable. These laws impose obligations regarding transparency, content moderation, and response to requests from authorities. Moreover, authorities responsible for the activities of SMPs have been established.

In contrast, in other countries, the legislation needed to regulate social media platforms is inadequate or non-existent. This leaves authorities without effective tools to compel platforms to take responsibility for hosted content and promptly respond to requests to remove harmful content.

In the **European Union**, the European External Action Service has been working since 2015 on tackling FIMI, including disinformation, and on strengthening its strategic communications in the Eastern Partnership, the Southern Neighbourhood, and the Western Balkans (EEAS 2024). To this end, the General Data Protection Regulation

(GDPR) - April 27, 2016 (EUR-Lex 2016), the Digital Services Act (DSA) - December 15, 2020 (EUR-Lex 2022b)[3], and the Digital Markets Act (DMA) - December 15, 2020 (EUR-Lex 2022a)[4] have been developed.

[3] Regulation (EU) 2022/2065 on a Single Market for Digital Services.
[4] Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector.

Germany has also shown interest in adapting legislation to current challenges. To this end, the **Network Enforcement Act (NetzDG)** was adopted in 2017 (bundesjustizamt.de 2018). Germany's NetzDG law is **one of the strictest regulations in Europe for combating online hate speech and disinformation**. The law obliges SMPs that have more than two million users in Germany to remove unlawful content within 24 hours or face fines of up to €50,000,000. While not solely focused on foreign disinformation, NetzDG plays a key role in preventing the spread of foreign-originated manipulative content

Meanwhile, Germany established the *National Cyber Defense Center*. This joint institution includes representatives from federal agencies, including the *Federal Office for Information Security* (BSI), the *Federal Intelligence Service* (BND), and the *Federal Office for the Protection of the Constitution* (BfV) – Germany's domestic intelligence agency. The Center coordinates Germany's response to cyber threats, which include FIMI and the use of cyber tools to spread disinformation.
The BfV has developed specialized programs to monitor FIMI in elections, particularly focusing on Russian and Chinese disinformation campaigns. Ahead of the 2021 federal elections, the BfV issued warnings and enhanced its monitoring of SMPs, and foreign-funded groups involved in spreading disinformation.

France adopted the 2018 *Law against the manipulation of information (Loi contre la manipulation de l'information)*, as a response to increasing concerns about FIMI in elections. Known as the "*Fake News Law*", it enables judges to act swiftly during elections by removing/blocking disinformation from media sources if it can be proven that they deliberately spread misleading information aimed at manipulating the outcome of an election. The law also requires SMPs to disclose their sponsors during election campaigns to avoid foreign-financed manipulation.

At the same time, *the Higher Audiovisual Council (Le Conseil Supérieur de l'Audiovisuel – CSA)*, France's media regulatory body has been granted enhanced powers to oversee media platforms and content dissemination. During election periods, the CSA can act against platforms that allow the spread of disinformation or manipulation originating from foreign actors. Furthermore, the CSA can impose sanctions on outlets that fail to meet transparency standards regarding political advertising.

For the regulation of social media platforms, the **US** makes use of Section 230 of the *US Communications Decency Act*, February 21, issued in 1996 (LLI 1996).
Starting with 2021, in **Australia** the *News Media Bargaining Code* is functioning.

In the **United Kingdom of Great Britain and Northern Ireland**, the *Online Safety Act 2023* was enacted (the Act) (GOV.UK 2023a). The Act is a set of strong regulations for protecting children and adults online. It contains new strict regulations for online SMPs and search engines, including obligations to protect users from harmful content, to quickly remove illegal content, to implement needed systems and processes for reducing risks related to their services when used for illegal/malicious activities, to take down illegal content as well criminal offenses. The law also contains provisions relating to *Ofcom* (the *Independent Regulator of Online Safety*), an entity involved in setting out the steps that providers can take to fulfill their safety duties in codes of practice, and has a broad range of powers to assess and enforce providers' compliance with the framework.

The Act's duties apply to search services/engines and services that are used to *allow users to post content online or to interact with each other*. This includes a range of websites, online instant messaging services, apps and other services, social media services, consumer file cloud storage and sharing sites, online forums, video-sharing platforms, and dating services. The Act applies to services linked to the UK, even if the companies providing them are outside the country (GOV.UK 2023b). The criminal offences introduced by the Act apply directly to the individuals sending them and cover: encouraging or assisting serious self-harm, cyberflashing, threatening communications, sending false information intended to cause non-trivial harm, intimate image abuse, epilepsy trolling.

The specific illegal content and activities, that platforms need to protect users from, are related to child sexual abuse, extreme sexual violence, controlling or coercive behavior, extreme pornography, fraud, inciting violence, racially, and religiously aggravated public order offenses, illegal immigration, and people smuggling, promoting or facilitating suicide, selling illegal drugs or weapons, intimate image abuse (revenge porn), sexual exploitation, terrorism. The Act also requires the platforms to rapidly remove illegal suicide and self-harm content and proactively protect users from content that is illegal under the *Suicide Act* from 1961.

The UK's *Counter Disinformation Unit* (CDU) was set up in 2019, being focused on monitoring the online content that poses risks to public health, public safety, and national security and responding to risks of misinformation, including that on Covid-19. CDU is involved in analyzing disinformation attempts and could work with social media companies to encourage them to promote authoritative sources of information. Currently, it is focused on disinformation related to Russia's illegal invasion of Ukraine and has already countered Russian disinformation about Ukraine. CDU has been talked about more than two hundred times in the British Parliament.

Canada operates the *Online Harms Bill*, which aims to tackle harmful online content, including hate speech, misinformation, and child sexual abuse.

Singapore enacted the 2019 Law for *Protection from Online Falsehoods and Manipulation Act* (POFMA) (Singapore.gov 2019). It allows the government to order the correction or removal of false/harmful information from SMPs.

Brazil is also paying attention to online activity, with the 2014 *Brazilian Civil Rights Framework for the Internet Law* (Secretaria-Geral 2014) that establishes principles for using the Internet in Brazil, including net neutrality and the protection of personal data.

In **India**, the Information Technology Rules (*Intermediary Guidelines and Digital Media Ethics Code*) or the "*IT Rules*" (Indian.gov 2021) came into effect in 2021 and laid down some specific compliance requirements for social media intermediaries. The *IT Rules* were introduced to check the spread of fake news, hate speech, and online harassment, some of the significant aspects being as follows:

- The SMPs/other intermediaries have to observe due diligence by making reasonable efforts to cause their users not to host, display, upload, modify, publish, transmit, store, update, or share any information that (1) is harmful to children (2) infringes the trademark, copyright, patent or other proprietary rights (3) is defamatory, obscene, invasive of the privacy of another person, is racially or ethnically objectionable (4) impersonates another person (5) violates any law.
- The rules provide an effective redressal mechanism by which users/victims may submit a complaint against IT Rules violations. The Grievance Officer must act in a time-bound manner after receiving a complaint in a request for the removal of information or communication link.
- It is mandatory for all significant SMPs to appoint a *Chief Compliance Officer* and a *Nodal Officer* who would be available 24*7 for coordination with law enforcement agencies.

In **Romania**, in May 2023, DNSC issued a recommendation to national state institutions and public bodies not to download, install, and use TikTok on their networks and information systems. At the same time, Romanian authorities are considering new legal provisions aimed at stricter regulations for social networks, creating a safer and more responsible online environment, designating national contact points/representatives for social networks in Romania, and introducing sanctions for non-compliance with content moderation obligations.

Conclusion

Online platforms and search engines allow users to develop global networks and are currently the most popular medium among content creators. The concept behind them seems innocuous, but the ease of access and the opportunities they offer also

involve some risks. Abuse of intellectual property, theft of personal and banking data, misinformation, spreading fake news, obscene content, violence, or hate speech are some of the challenges.

Both malicious activities conducted on SMPs by state and non-state actors and other forms of foreign interference constitute a threat to democratic principles and values, having a negative impact on national security, democracy, state institutions, critical infrastructure, society, business, and citizens. Some of those most exposed to harmful and inappropriate online content are children, women, girls, but also the elderly.

This scientific research attests that both ordinary users and national authorities face problems related to the lack of a legal regulatory framework, formal procedures, or the possibility to directly contact representatives of social media platforms when needed to take action to block/remove/modify such illegal activities or inappropriate messages in a timely manner. The study also notes several complaints of lack of adequate response from MSPs to user reports and requests to block/remove attack vectors.

On the other hand, SMPs face ongoing challenges in moderating the illegal content published online. Some of them have implemented various measures to address these issues (content moderation; increasing transparency around content moderation; improving algorithms to automatically detect harmful content; classifying content; acting on the resulting classifications; and working with fact-checkers), but they are often insufficient and slow to respond to requests to remove harmful content. This is partly due to the large volume of user-generated content, but also due to a lack of sufficient incentives and penalties to act quickly and efficiently.

The time has come for SMPs to recognize their responsibility, invest in robust security measures, proactively tackle this, and prioritize the safety of their users in the digital age. Legal obligations should be brought to the attention of all audio-visual broadcasters and social media platforms to provide the public with unbiased and objective information, presenting facts and events accurately, while respecting the freedom of expression.

After this present study, a main conclusion could be drawn: **countries need effective regulatory frameworks and policies for making the use of Internet services safer**. They should be applied to **social media platforms, search engines, and services that allow users to post content online or to interact with each other**: a range of websites, online instant messaging, online forums, services apps, and other services, including social media services, consumer file cloud storage and sharing sites, video sharing platforms, dating services, etc. The legislation should be balanced, protect freedom of expression, but also ensure that online platforms take responsibility for the content they host and contribute to a safer and healthier online environment, to protect users from harmful content, quickly remove illegal content, implement

systems and processes necessary to mitigate the risks of the services offered when used for malicious activities.
In light of the current context and international experience, countries around the world could consider taking legislative action in the following areas to better regulate social media platforms, search engines, and services that allow users to post social content online, and to protect them.

Looking at the current framework, **transparency and accountability** of online platforms are essential elements. They should appoint a national representative in the countries where they operate, responsible for communicating with the authorities and ensuring compliance with local legislation. Users also need simple and accessible mechanisms to report harmful content and/or challenge moderation decisions. At the same time, online platforms should regularly publish detailed reports on the measures taken to moderate content, the number of complaints received, and how they have been resolved.

In terms of **content moderation**, social media platforms, search engines, and services that allow users to post content online or interact with each other should be obliged to remove illegal content within a short period of notice. They also need to work better with independent fact-checking organizations and human rights experts to improve content moderation. On the other hand, platforms should be encouraged to use advanced technologies such as artificial intelligence to quickly identify and automatically remove harmful content.

Regarding **user protection**, it is important to implement specific measures to protect children from harmful content, such as age restrictions and parental control tools. SMPs should take effective measures to limit the spread of misinformation, with an emphasis on labeling false or misleading content and promoting credible sources of information. Personal data protection legislation must be strictly enforced, and users must be in control of how their data is collected and used.

To support these measures, **supervisory and regulatory bodies need to be established**. Such bodies are needed to oversee the activity of social media platforms, search engines, and services that allow users to post content online or interact with each other. They should also be empowered to act against companies or platforms that allow FIMI or other illegal activities to take place online, and to impose sanctions for violations of the laws and rules imposed.

In terms of **sanctions**, online platforms that do not comply with legal obligations should be subject to fines, proportionate to the seriousness of the infringement and the company's turnover. In particular cases, the national authorities should have the possibility to temporarily suspend or block the services provided by online platforms and search engines, whenever the situation so requires.

References

Adrien, Claudia. 2023. ”Phishing Attacks Target Facebook, Microsoft, Making Them Most Impersonated Brands”. https://www.channelfutures.com/security/phishing-attacks-target-facebook-microsoft-making-them-most-impersonated-brands.

Alexander, Brooke Nelson. 2022. ”What Is Doxxing, and How Does It Set You Up to Be Hacked?” https://www.rd.com/article/what-is-doxxing/.

—. 2023. ”What Is Spoofing, and How Can You Spot It?”. https://www.rd.com/article/spoofing/.

—. 2024. ”14 Facebook Marketplace Scams to Watch Out For”. https://www.rd.com/article/facebook-marketplace-scams/.

Baiaș, Ionuț. 2023. „Directoratul Național de Securitate Cibernetică recomandă interzicerea TikTok pe dispozitivele instituțiilor publice”. https://hotnews.ro/directoratul-national-de-securitate-cibernetica-recomanda-interzicerea-tiktok-pe-dispozitivele-institutiilor-publice-64785.

Bradford, Alina. 2024. ”8 Common Bank Scams to Watch Out For”. https://www.rd.com/list/bank-scams/.

Budgar, Laurie. 2024. ”Can You Really See Who Viewed Your Facebook Profile Recently?”. https://www.rd.com/article/who-viewed-my-facebook-profile/.

bundesjustizamt.de. 2018. ”Network Enforcement Act Regulatory Fining Guidelines”. https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/NetzDG/Leitlinien_Geldbussen_en.pdf?__blob=publicationFile&v=3.

Chin, Kyle. 2024. ”19 Most Common Types of Phishing Attacks in 2024”. https://www.upguard.com/blog/types-of-phishing-attacks.

Comisia Europeană. 2024. ”Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain”. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2227.

DNSC. 2023a. „ALERTA: Tentative de fraudă promovate prin anunțuri sponsorizate pe rețelele sociale”. https://www.dnsc.ro/citeste/alerta-tentative-de-frauda-promovate-prin-anunturi-sponsorizate-social-media.

—. 2023b. ”Press release.” https://dnsc.ro/vezi/document/comunicat-de-presa-dnsc-recomanda-autoritatilor-si-institutiilor-publice-din-romania-interzicerea-descarcarii-instalarii-si-utilizarii-a-aplicatiei-tiktok-pe-dispozitivele-de-serviciu-pdf.

EEAS. 2024. ”Tackling Disinformation, Foreign Information Manipulation & Interference”. https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.

EUR-Lex. 2016. ”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”. https://eur-lex.europa.eu/eli/reg/2016/679/oj.

—. 2022a. "Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector". https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32022R1925.

—. 2022b. "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services". https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

Giles, Keir. 2016. "Handbook of Russian Information Warfare". https://www.ndc.nato.int/news/news.php?icode=995.

Gordon, Anna. 2024. "Here's All the Countries With TikTok Bans as Platform's Future in U.S. Hangs In Balance". https://time.com/6971009/tiktok-banned-restrictions-worldwide-countries-united-states-law/.

GOV.UK. 2023a. "Online Safety Act 2023." https://www.legislation.gov.uk/ukpga/2023/50/enacted.

—. 2023b. "What the Online Safety Act does." https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer#:~:text=The%20Online%20Safety%20Act%202023,users'%20safety%20on%20their%20platforms.

Hindman, Matthew. 2018. "Disinformation, 'Fake News' and Influence Campaigns on Twitter." https://knightfoundation.org/reports/disinformation-fake-news-and-influence-campaigns-on-twitter/.

Indian.gov. 2021. "The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)." https://www.meity.gov.in/writereaddata/files/Information%20Technology%20%28Intermediary%20Guidelines%20and%20Digital%20Media%20Ethics%20Code%29%20Rules%2C%202021%20%28updated%2006.04.2023%29-.pdf.

ITU. 2021. "Session 5: Disinformation, misinformation, malinformation and Infodemics: Ways to handle". https://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Pages/Events/2021/ASP%20Regional%20Dialogue%20on%20Digital%20Transformation/Session%20Pages/RD-Session-5.aspx.

Justia. 2021. "Gonzalez v. Google, LLC, No. 18-16700 (9th Cir. 2021)." https://law.justia.com/cases/federal/appellate-courts/ca9/18-16700/18-16700-2021-06-22.html.

Lakshmanan, Lavie. 2024. "Canada orders TikTok to shut down Canadian operations over security concerns". https://thehackernews.com/2024/11/canada-orders-tiktok-to-shut-down.html?m=1.

LLI. 1996. "47 U.S. Code § 230 – Protection for private blocking and screening of offensive material." https://www.law.cornell.edu/uscode/text/47/230.

PakVoices. 2023. "Disinformation impacts on digital sphere in Pakistan (May-July 2023)." https://pakvoices.pk/?p=13745.

Petkauskas, Vilius. 2023. "Facebook Messenger phishing attack pumps out 100K+ weekly messages". https://cybernews.com/news/facebook-messenger-phishing-attack/.

Qureshi, Anees. 2023. "Meta Neglecting the Proliferation of Phishing Scam Pages on Facebook, Leaving Millions of Users Vulnerable". https://www.linkedin.com/pulse/meta-neglecting-proliferation-phishing-scam-pages-facebook-qureshi-dsizf/.

Rosenkrantz, Holly. 2024. "What Is Phishing, and How Can You Prevent This Cyberattack?". https://www.rd.com/article/what-is-phishing/.

Saint Francis University. 2023. "Misinformation, Disinformation, and Fake News". https://libguides.francis.edu/fake-news.

Sasnauskas, Mantas. 2023. "We uncovered a Facebook phishing campaign that tricked nearly 500,000 users in two weeks". https://cybernews.com/security/we-uncovered-a-facebook-phishing-campaign-that-tricked-nearly-500000-users-in-two-weeks/.

Schappert, Stefanie. 2024. "Meta deletes 63K sextortion scam accounts from Instagram, Facebook".https://cybernews.com/news/meta-deletes-63k-sextortion-scam-accounts-instagram-facebook/.

Secretaria-Geral. 2014. "LEI Nº 12.965, DE 23 DE ABRIL DE 2014." http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm.

Singapore.gov. 2019. "Protection from Online Falsehoods and Manipulation Act 2019." https://sso.agc.gov.sg/Act/POFMA2019.

Snegovaya, Maria. 2015. "Putin's Information Warfare in Ukraine: Soviet Origins of Russia's Hybrid Warfare, Institute for the Study of War." https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare.

Stathis, Jaime. 2024a. "14 Online Scams You Need to Be Aware Of—and How to Avoid Them". https://www.rd.com/list/how-to-avoid-online-scams/.

—. 2024b. "9 Red Flags You're About to Click on a Fake Social Media Ad". https://www.rd.com/list/fake-ads-on-social-media/.

Toulas, Bill. 2023a. "Facebook disrupts new NodeStealer information-stealing malware." https://www.bleepingcomputer.com/news/security/facebook-disrupts-new-nodestealer-information-stealing-malware/.

—. 2023b. "Facebook Messenger phishing wave targets 100K business accounts per week". https://www.bleepingcomputer.com/news/security/facebook-messenger-phishing-wave-targets-100k-business-accounts-per-week/.

Zaleznik, Daniel. 2021. "*Facebook and Genocide: How Facebook contributed to genocide in Myanmar and why it will not be held accountable*". https://systemicjustice.org/article/facebook-and-genocide-how-facebook-contributed-to-genocide-in-myanmar-and-why-it-will-not-be-held-accountable/.

Zaytsev, Oleg. 2023. "«MrTonyScam» — Botnet of Facebook Users Launch High-Intent Messenger Phishing Attack on Business Accounts". https://labs.guard.io/mrtonyscam-botnet-of-facebook-users-launch-high-intent-messenger-phishing-attack-on-business-3182cfb12f4d.

BULLETIN
OF "CAROL I" NATIONAL DEFENCE UNIVERSITY

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

Increasing the cyber resilience of SMEs through open-source solutions and international collaboration

Ionica ȘERBAN, Ph.D.*
Florentina-Mihaela CURCĂ, M.S.**
Robert-Ștefan ȘANDRU, M.S.***

*Romanian National Cyber Security Directorate
e-mail: ionica.serban@dnsc.ro
**Romanian National Cyber Security Directorate
e-mail: mihaela.curca@dnsc.ro
***Romanian National Cyber Security Directorate
e-mail: robert.sandru@dnsc.ro

Abstract

In an increasingly digitalized world, small and medium-sized enterprises (SMEs) are exposed to significant cyber threats due to limited security resources. This article explores the role of open-source solutions and international collaboration in enhancing the cyber resilience of SMEs. Open-source solutions offer financial accessibility, flexibility, and increased security, supported by global communities that contribute to their continuous improvement. Moreover, decentralized sharing of threat information, combined with artificial intelligence, enables more efficient detection and prevention of cyberattacks. Through collaborative initiatives such as HackOlympics, SMEs can learn through hands-on experience and benefit from solutions tested in real-life scenarios. In conclusion, open-source solutions and the use of advanced technologies, such as AI, provide SMEs with an effective strategy to address modern cyber challenges, improving their resilience and protection against threats.

Keywords:
cybersecurity; SMEs; open-source solutions; international collaboration; artificial intelligence; HackOlympics.

Article info
Received: 15 August 2024; Revised: 10 September 2024; Accepted: 24 September 2024; Available online: 15 October 2024

Citation: Șerban, I., F.M. Curcă și R.Ș. Șandru. 2024. "Increasing the cyber resilience of SMEs through open-source solutions and international collaboration". *Bulletin of "Carol I" National Defence University*, 13(4): 266-286. https://doi.org/10.53477/2284-9378-24-63

In the era of accelerated digitalization, cybersecurity has become a global challenge, affecting all types of organizations, regardless of size. However, small and medium-sized enterprises (SMEs) are particularly vulnerable, as they often lack the necessary resources to invest in advanced protection technologies and to implement robust security systems. These companies represent an essential segment of the global economy, contributing significantly to economic development, innovation, and employment. Despite this, many SMEs are attractive targets for cyber attackers, as they often hold valuable data but have underdeveloped security infrastructures.

SMEs face a series of unique challenges regarding cybersecurity. First, the lack of financial and human resources limits their ability to invest in expensive commercial cybersecurity solutions, which are more accessible to large companies. Secondly, SMEs lack dedicated teams or expertise in cybersecurity, making them less prepared to quickly detect and respond to cyber threats.
Additionally, SMEs are often focused on business growth and do not perceive cyber risks as a priority, leading to a lack of proactive measures to prevent attacks. This puts them in a vulnerable position, frequently suffering from attacks such as ransomware, phishing, and data breaches, which can cause substantial financial losses, damage reputation, and erode customer trust.

Open-source solutions are an accessible alternative and provide a viable option for SMEs to strengthen their cybersecurity. These solutions offer free access to advanced technologies that can be adapted and customized according to each organization's needs. Moreover, open-source communities are highly active in addressing vulnerabilities and continuously improving these solutions, allowing SMEs to benefit from the latest innovations and practices in cybersecurity.
Adopting these solutions does not require significant initial costs, and SMEs can choose to gradually implement security measures as they develop their capacities and resources. Additionally, open-source solutions offer a high level of transparency and flexibility, allowing for deeper customization and easy integration into the existing systems of SMEs.

Another crucial aspect of enhancing the cyber resilience of SMEs is international collaboration. Cyberattacks are global in nature, and to combat these complex threats, SMEs must engage in information-sharing networks, collaborate with other companies and institutions in the security field, and learn from the experiences of other entities worldwide.

Collaboration between SMEs and international organizations allows for the exchange of best practices and access to educational resources, conferences, hackathons, and attack simulations. This creates a mutually supportive ecosystem where new threats are quickly identified, and solutions are developed and distributed to the community, thereby increasing SMEs' ability to respond swiftly to risks and improve their defence systems.

Although SMEs are vulnerable due to limited resources, they have the opportunity to enhance their cyber resilience by adopting open-source solutions and participating in international collaboration initiatives. These measures, along with continuous education and awareness of the importance of cybersecurity, will enable SMEs to face the challenges of today's digital environment, ensuring their long-term protection and contributing to the stability and development of the global economy.

Methodology

The scientific method used in this paper focuses on an integrated and multidisciplinary approach to evaluate the effectiveness of open-source solutions in increasing the cyber resilience of SMEs. The methodology was structured into several stages to ensure a comprehensive and rigorous analysis of the subject. The first stage involved a systematic review of existing literature to understand the current cybersecurity landscape and the use of open-source solutions by SMEs. Academic sources and industry reports were utilized to identify the challenges and needs of SMEs in terms of cybersecurity. Databases such as IEEE Xplore, Google Scholar, and Scopus were used to extract relevant articles on security technologies, artificial intelligence, and threat information sharing.
Next, a comparative analysis of the open-source solutions available for SMEs, such as OpenVAS, Suricata, and PfSense, was conducted. This stage involved evaluating these solutions based on key criteria, including costs, ease of use, flexibility, and effectiveness in threat detection and prevention.

This paper stands out through its in-depth study of the impact of open-source solutions on the cybersecurity of small and medium-sized enterprises (SMEs), a topic of growing interest in the era of digitalization. In this context, solutions such as OpenVAS, Suricata, and PfSense play a crucial role, increasingly adopted by SMEs seeking efficient and affordable alternatives to commercial solutions.

According to a recent report by the Ponemon Institute (2023), over 45% of SMEs globally use at least one open-source solution for cybersecurity. Of these, 60% cite financial accessibility as the primary reason for adopting such solutions. Specifically, OpenVAS, a platform for vulnerability assessment, is utilized by approximately 35% of SMEs implementing open-source solutions. This platform enables companies to quickly identify weaknesses in their IT infrastructure, reducing the risk of critical vulnerabilities being exploited.

Additionally, Suricata, an advanced solution for intrusion detection and prevention, is integrated into the security systems of SMEs worldwide. According to a study published by OWASP (2023b), the use of Suricata has increased by 50% over the past two years, with SMEs appreciating its real-time monitoring capabilities and adaptability to various types of cyberattacks.

PfSense, an extremely popular open-source firewall solution, has proven to be an essential tool for SMEs. Data provided by the PfSense project indicate that over 70% of its users are small and medium-sized organizations, with implementations leading to cost savings of up to 80% compared to commercial solutions. Furthermore, a Gartner report Gartner (2023) highlights that SMEs using PfSense experience significant improvements in network security due to the flexibility and ease of customization this solution provides.

In the case study presented in this article, an SME from the IT sector in Romania implemented PfSense to address security challenges. Following this implementation, the company managed to reduce cyberattacks by 80% and ensure robust operational continuity while keeping costs at a minimum. These results support global trends and demonstrate that SMEs can leverage open-source solutions to strengthen their cybersecurity resilience without being constrained by large budgets.

The integration of these statistics and data highlights the practical relevance of open-source solutions in protecting SMEs against cyber risks and underscores the significant contribution of this paper in promoting the use of such technologies. Thus, the paper not only demonstrates the applicability of these solutions but also provides a concrete framework for analysis and implementation, based on current trends and the actual needs of small and medium-sized enterprises.

Security Challenges for SMEs in the Digital Era

Small and medium-sized enterprises (SMEs) are the backbone of European economies, accounting for approximately 99% of all businesses and generating two-thirds of jobs in Europe (European Commission 2023). However, they face major cybersecurity challenges as digitalization becomes essential for the operation of modern businesses. The lack of financial resources and in-house expertise limits SMEs' ability to invest in advanced security technologies, leaving them vulnerable to cyberattacks (ENISA 2023c).
In an era where cybercrime is rapidly evolving, SMEs are increasingly becoming the target of attacks. Studies show that over 60% of cyberattacks target SMEs (Verizon 2023), which are seen as easier targets due to the lack of protective measures compared to large corporations.

Phishing is one of the most widespread threats. SME employees receive fraudulent emails that claim to be from legitimate organizations, attempting to obtain sensitive data. This type of attack accounts for nearly 57% of all security incidents reported among SMEs.
Ransomware has become an omnipresent threat, with SMEs frequently targeted due to the lack of adequate backup solutions. Ransomware encrypts a company's data and demands a ransom to unlock access. It is estimated that 43% of ransomware attacks target SMEs.

DDoS (Distributed Denial of Service) attacks disrupt a company's online services by flooding servers with fake traffic, which can severely impact SME operations, especially those that rely on online functionality (Arbor Networks 2023).
Data breaches represent a major threat, especially for SMEs that handle sensitive data. Studies show that 60% of SMEs that suffer major security breaches shut down within six months. The financial impact of a breach can be devastating, considering the recovery costs and legal penalties that may arise from non-compliance with data protection regulations, such as GDPR.

One of the main factors contributing to the vulnerability of SMEs is the lack of financial resources. Advanced security solutions are often expensive, and SMEs have limited budgets to purchase and implement them. According to a 2023 report, 60% of SMEs cannot afford to invest in commercial security solutions (Gartner 2023).
The lack of internal expertise is another significant obstacle. Most SMEs do not have dedicated cybersecurity staff and rely on small IT teams or even non-technical personnel to manage security issues. This lack of expertise leads to inadequate preparedness against attacks and slow responses to incidents (NIST 2022a).

Outdated infrastructures are another major problem for SMEs. Many of them use old, unsecured technologies without implementing regular security patches. This situation leaves open doors for attackers who exploit known vulnerabilities.
Reduced risk awareness is also an important factor. Many SME managers underestimate cyber risks, believing that their business is not large or valuable enough to attract attacks. This misconception prevents SMEs from taking proactive measures to prevent attacks.

Cyberattacks can have devastating consequences for SMEs, which often lack the resources to recover quickly. The financial losses generated by these attacks can include ransom payments, business losses due to service disruptions, and additional costs for data recovery.
Moreover, the reputational impact of an attack can be equally damaging. A security breach can severely undermine the trust of customers and business partners, especially if their data is compromised. In an era where personal data protection is a priority, such an incident can lead to customer loss and financial penalties imposed by regulations such as GDPR.

One of the fundamental challenges for SMEs in ensuring cybersecurity is the accessibility and scalability of solutions. Unlike large corporations that can allocate significant budgets for the implementation of advanced security solutions, SMEs operate with limited financial and human resources. For this reason, traditional and commercial security solutions are often financially inaccessible, and their complexity can exceed the capabilities of the limited technical teams these companies have.
Commercial, enterprise-level security solutions, such as advanced firewalls, intrusion prevention systems (IPS), backup and disaster recovery solutions, or identity and

access management (IAM) systems, are generally developed for large organizations that have the resources to implement and maintain them. These solutions not only involve high initial costs but also recurring expenses for licenses, technical support, and regular updates. For SMEs, these costs represent a significant burden, making it difficult for many of them to afford such investments (Verizon 2023).

Additionally, many commercial solutions are designed for complex infrastructures and organizations with diverse needs, making it difficult to adapt to the needs of an SME. Limited technical staff and, often, the lack of a dedicated IT department means that many SMEs cannot manage complex solutions, leaving them vulnerable to cyberattacks.

In this context, open-source solutions have gained ground as a viable alternative for SMEs. Open-source solutions, developed and supported by global communities of developers and security specialists, are freely available, offer high flexibility, and give SMEs the ability to tailor them to their specific needs (OWASP 2023a).
Examples of open-source solutions used in cybersecurity include:

- OpenVAS (Open Vulnerability Assessment System) for vulnerability scanning;
- Suricata and Snort for intrusion detection and prevention;
- PfSense for firewalls and routers;
- ClamAV for protection against viruses and malware.

These solutions are accessible to SMEs not only due to their low cost (most are free) but also because of the broad support provided by the communities around these projects, which contribute to frequent updates and vulnerability fixes.
Another major advantage of open-source solutions is scalability. For SMEs, which are continuously evolving, it is essential that security solutions can grow alongside the business. Open-source solutions can be initially configured to cover basic security needs, and as the business expands, these solutions can be scaled without significant costs.

For example, an open-source firewall like PfSense can initially be implemented on a small scale to manage network traffic and can later be expanded to cover larger networks or include advanced functionalities such as VPNs or QoS (Quality of Service), without incurring major additional costs for licensing or hardware (PfSense Project 2023). Moreover, open-source solutions allow SMEs to customize their configurations to meet specific needs, making them far more flexible compared to commercial solutions (NIST 2022b).

Another important aspect that makes open-source solutions attractive to SMEs is the active support from global communities. Open-source platforms benefit from constant contributions from developers and security experts worldwide, who continuously improve functionalities and identify new vulnerabilities.

In addition to technical contributions, these communities also offer educational support through forums, guides, and tutorials, helping SMEs understand and correctly implement open-source solutions. As a result, SMEs do not have to rely on commercial vendors for technical support, significantly reducing long-term costs.

In conclusion, open-source solutions offer SMEs a viable, accessible, and scalable alternative for cybersecurity protection. These solutions not only provide high-quality technology without prohibitive costs but also allow for quick adaptation to the needs of growing organizations. Moreover, the support provided by international communities and the flexibility of open-source solutions ensure that SMEs can face cyber challenges with limited resources, thus contributing to the enhancement of their cyber resilience.

Legislative, Normative, and Strategic Aspects of International Collaboration

International collaboration in cybersecurity represents a fundamental pillar in protecting small and medium-sized enterprises (SMEs) against increasingly sophisticated cyber threats. In a digitalized world where attacks transcend national borders, SMEs benefit not only from open-source technologies but also from a legislative, normative, and strategic framework designed to support them in addressing global challenges. This chapter explores how international initiatives, global standards, and coordinated strategies can enhance the cybersecurity resilience of SMEs.

At the European level, the European Union has developed a set of essential regulations encouraging SMEs to adopt proactive cybersecurity measures. The NIS2 Directive, a central element in this landscape, sets high protection standards for companies operating in sectors considered essential. SMEs are required to implement measures such as:

- Developing policies for managing cybersecurity risks.
- Promptly reporting cyber incidents to the competent authorities.
- Collaborating in information-sharing networks about threats.

The European Union Agency for Cybersecurity (ENISA) supports these efforts by providing practical guidelines, simulation exercises, and tools tailored for SMEs. A notable example is the organization of European-scale cyber simulations, enabling SMEs to test and improve their defence strategies under realistic conditions.

Adopting international standards, such as ISO/IEC 27001, offers SMEs a globally recognized framework for managing information security. These standards not only establish a clear set of best practices but also:

- Reduce risks through validated control measures.

- Enhance trust among clients and partners.
- Facilitate compliance with legislative requirements in various countries.

For SMEs, adopting ISO/IEC 27001 can become a competitive advantage, opening access to international markets and consolidating their reputation as trusted partners.

A crucial element of international collaboration is the sharing of information on cyber threats. Platforms such as MISP (Malware Information Sharing Platform) or STIX/TAXII allow SMEs to access up-to-date data on attacks, techniques, and tactics used by malicious actors. This information-sharing process offers multiple benefits:

- Rapid identification of emerging threats.
- Mutual support among companies and industrial sectors.
- Creation of a stronger collective defence.

For example, by participating in these platforms, SMEs can prevent ransomware attacks that impact supply chains, thus protecting not only their business but also their partners.

In addition to European initiatives, organizations such as the Organization for Economic Cooperation and Development (OECD) and the World Economic Forum contribute to promoting global collaboration in cybersecurity. These organizations:

- Develop policies supporting SMEs in adopting efficient cybersecurity solutions.
- Provide educational resources to raise cybersecurity awareness.
- Facilitate the exchange of best practices across sectors and regions.

A concrete example is the Forum of Incident Response and Security Teams (FIRST), which facilitates cooperation among organizations worldwide, including SMEs, to coordinate responses to cyber incidents.

International regulations, such as the General Data Protection Regulation (GDPR), require SMEs to adopt strict measures for protecting personal data. Simultaneously, international treaties and partnerships in cybersecurity enable SMEs to benefit from cross-border support. These legislative frameworks provide SMEs with the tools necessary to navigate a complex and dynamic environment.

Integrating legislation, global standards, and international strategies offers SMEs a holistic approach to managing cybersecurity risks. By combining open-source technologies with these normative and strategic instruments, SMEs can build a resilient ecosystem capable of addressing contemporary digital challenges.

International collaboration extends beyond technological exchanges; it involves a coordinated commitment between legislation, norms, and global strategies to support SMEs in facing cyber threats. European initiatives, ISO standards, and information-sharing platforms provide SMEs with the resources needed to navigate successfully in the digital landscape. By adopting these measures, SMEs not only protect their businesses but also contribute to strengthening a global security environment built

on cooperation and trust. This integrated vision transforms SMEs from vulnerable targets into proactive actors within the global cybersecurity ecosystem.

Open-Source Solutions for the Cybersecurity of SMEs

Open-source solutions represent a viable and efficient alternative for SMEs when it comes to cybersecurity. These solutions have gained popularity in recent years due to their flexibility, accessibility, and the active communities that contribute to their continuous development and improvement. For SMEs, which face budget constraints and limited technical resources, open-source solutions offer several significant advantages.

One of the greatest benefits of open-source solutions is financial accessibility. Unlike commercial solutions, which can involve high costs for licensing, support, and maintenance, open-source solutions are usually free or available at a very low cost. This makes open-source solutions attractive for SMEs, which typically do not have large budgets for cybersecurity.

This chapter provides a concise overview of the main open-source solutions relevant to SMEs, such as **PfSense, Suricata**, and **OpenVAS**, highlighting their benefits and applicability.

PfSense – Network Protection Through an Accessible Firewall

PfSense is an open-source firewall solution that offers SMEs an affordable and flexible way to secure their IT networks. This technology is appreciated for the following features:

- Allows detailed rule configuration for managing network access.
- Provides a secure environment for remote access to resources, essential for companies with remote-working employees.
- Enables SMEs to start with a basic configuration and add additional functionalities as the business grows.

According to a Gartner report (2023), over 70% of SMEs using PfSense report significant improvements in network security and a considerable reduction in operational costs.

Suricata – Advanced Intrusion Detection

Suricata is an open-source solution specializing in intrusion detection and prevention (IDS/IPS) and is widely used for network traffic monitoring. It offers SMEs the ability to:

- Identify suspicious network activities and block threats before they cause damage.
- Be configured to meet the specific needs of each company.
- Easily integrate with other open-source solutions, providing a comprehensive protection system.

OWASP studies (2023) indicate that the use of Suricata in SMEs has increased by 50% in recent years, thanks to its ability to detect emerging threats and offer protection against complex cyberattacks.

OpenVAS – Vulnerability Assessment

OpenVAS (Open Vulnerability Assessment System) is an open-source tool that helps SMEs identify and remediate vulnerabilities in their IT infrastructure. It stands out for:

- Detecting weaknesses in IT systems and providing detailed reports to prioritize remediation.
- Ensuring regular security assessments, preventing the exploitation of unknown vulnerabilities.
- Being free to use and offering extensive support from user and developer communities.

According to the Ponemon Institute (2023), OpenVAS is used by 35% of SMEs that have implemented open-source solutions, helping reduce security risks by proactively identifying vulnerabilities.

PfSense, Suricata, and **OpenVAS** are essential tools for SMEs seeking to enhance their cybersecurity resilience without major investments. Each solution provides specific functionalities that can be easily integrated into a comprehensive security strategy tailored to the needs of individual SMEs. Thanks to their financial accessibility, ease of use, and support from global communities, these open-source solutions become optimal choices for small and medium-sized organizations facing increasingly complex challenges in the digital environment (OWASP 2023a).
Moreover, recurring costs, such as those for support and maintenance, are significantly reduced, as open-source communities offer free updates and a wide range of educational resources.

Open-source solutions are extremely flexible and can be customized according to the specific needs of an organization. This is essential for SMEs, which have varied security requirements and cannot justify the implementation of rigid, standardized solutions available on the commercial market. With open-source solutions, companies can adapt functionalities to their own IT infrastructures and available resources.
For example, SMEs can choose to implement only certain modules of an open-source solution, such as a simple firewall or an intrusion detection system, and add other functionalities as the business and technical infrastructure grow (PfSense Project 2023). This scalability allows SMEs to expand without being constrained by predefined and expensive commercial solutions.

Another significant benefit of open-source solutions is the active support provided by global communities of developers and cybersecurity experts. These communities

continuously contribute to the development and improvement of open-source solutions, ensuring quick updates and timely vulnerability fixes.
For instance, platforms like GitHub or Stack Overflow are widely used by open-source developers to share code, solutions, and best practices, facilitating collaboration between SMEs and international experts. This free community support offers SMEs extensive access to technical assistance resources without having to pay for costly commercial support contracts.

Another key advantage of open-source solutions is code transparency. The source code is open, meaning it can be analyzed and reviewed by anyone, including security specialists. This transparency allows for an objective and detailed assessment of potential security vulnerabilities before they are exploited.
Additionally, developers and users can contribute to improving security by quickly reporting bugs and creating patches that are available to the entire community. This collaborative model is much more agile than the update cycles of commercial solutions, which can take months or even years to officially address vulnerabilities.

Using open-source solutions gives SMEs independence from commercial vendors, eliminating vendor lock-in or restrictive contracts. With commercial solutions, SMEs often have to rely on a specific vendor for updates, support, and maintenance, which can limit their long-term options and increase costs.
In contrast, open-source solutions allow SMEs to be autonomous, manage their security internally, and collaborate with various community resources to customize and update the solutions as their needs evolve.

The **HackOlympics initiative** is an international cybersecurity platform dedicated to the collaborative testing and development of security solutions through the involvement of the ethical hacker community and security experts worldwide. This initiative is based on the principle of "collaborative learning" and promotes the testing and improvement of cybersecurity solutions in an open, transparent, and competitive framework. HackOlympics brings together teams of specialists who test their skills in a controlled environment, replicating real-world cyberattack and defence scenarios.

One of the main objectives of HackOlympics is to create a global cybersecurity community that collaborates to find innovative and accessible solutions to current security problems. Through competitions and practical exercises, participants are challenged to develop real-time solutions based on simulated attack scenarios that reflect contemporary cyber threats.
This approach offers SMEs a unique advantage: the opportunity to learn from real-world experiments and benefit from solutions tested by experts from around the world. The platform allows SMEs to implement solutions that have been validated in public competitions, giving them increased confidence in the effectiveness of these technologies (SANS Institute 2023).

Collaborative learning is a central component of HackOlympics, bringing together participants from various regions and organizations to collaborate and share knowledge in the field of cybersecurity. This global collaboration facilitates the exchange of best practices and offers a platform for continuous testing of open-source solutions.
One of the main advantages of this type of collaborative learning is the ability to address new or emerging vulnerabilities in a very short time. Participants work together to identify weaknesses in open-source solutions and develop patches or fixes at an accelerated pace. In this way, HackOlympics contributes to the constant improvement of SMEs' cyber resilience, giving them access to solutions that have been tested in the most challenging conditions.

For SMEs, involvement in HackOlympics or using solutions developed and tested within this platform brings several significant benefits:

- **Access to high-quality solutions:** The solutions tested in HackOlympics are subjected to complex simulated attacks, ensuring that the technologies used by SMEs are robust and efficient.
- **Cost reduction:** By collaborating with global communities and adopting tested open-source solutions, SMEs can significantly reduce the costs associated with purchasing and maintaining commercial security solutions**.**
- **Improved incident response capacity:** HackOlympics participants learn how to quickly detect and respond to various cyber threats, enabling SMEs to adopt more effective incident response protocols.

International collaboration is essential in the context of global cybersecurity, as attacks do not respect national borders, and cyber attackers are often organized internationally. HackOlympics facilitates this type of collaboration by bringing together experts and ethical hackers from diverse cultures and regions to find solutions to common security problems.
In addition, HackOlympics contributes to the continuous education of cybersecurity professionals, including those from SMEs, by organizing workshops, conferences, and training sessions. These events offer an open platform for knowledge exchange and skill development, thereby helping to raise the global level of expertise in cybersecurity.

HackOlympics represents an example of an innovative initiative that improves global cybersecurity through collaboration and continuous learning. SMEs directly benefit from these competitions by gaining access to solutions tested and verified by international experts, enabling them to increase their cyber resilience and reduce security-related costs. Collaborative learning and the exchange of best practices are key to developing effective and accessible solutions in the face of increasingly complex cyber threats.
In conclusion, open-source solutions offer SMEs a wide range of advantages, enabling them to ensure cybersecurity without being burdened by significant costs

or technological constraints. Accessibility, flexibility, community support, and code transparency make these solutions an optimal choice for SMEs, allowing them to improve their cyber resilience in a scalable and efficient manner.

The Role of Artificial Intelligence in Enhancing Cybersecurity

Artificial intelligence (AI) plays an increasingly important role in cybersecurity, providing new methods for proactive detection and prevention of cyberattacks. AI-based technologies enable the rapid and precise identification of threats, the analysis of unusual network behaviour, and the detection of advanced cyberattacks, such as zero-day exploits and Advanced Persistent Threats (APT) (ENISA 2023a). In a context where the volume and complexity of attacks are increasing, SMEs can significantly benefit from the use of AI to improve their cyber resilience.

One of the most powerful applications of AI in cybersecurity is the detection of anomalies in networks and systems. Machine learning algorithms can analyze large volumes of data and identify behavioural patterns that indicate potential attacks. Unlike traditional systems, which rely on predefined rules to detect threats, AI can learn and adapt in real-time to recognize new behaviours or anomalies in network traffic.

For example, AI-based intrusion detection systems, such as those offered by open-source solutions like Suricata, use machine learning algorithms to detect deviations from normal user behaviour and prevent security breaches before they can be exploited. By continuously monitoring and analyzing suspicious behaviour, AI can detect cyber threats in real-time, giving SMEs a significant advantage over attackers.

In addition to anomaly detection, AI plays an important role in attack prevention by using predictive algorithms. These algorithms can analyze historical data and previous attack patterns to anticipate potential future threats (Symantec 2023). For instance, machine learning algorithms can analyze security logs and identify specific patterns that indicate a possible ransomware or phishing attack.

These predictive methods are essential for SMEs because they enable proactive interventions before attacks occur. Unlike traditional solutions that focus only on responding to attacks once they have started, AI allows for threat anticipation and prevention, thereby reducing risks and damages for SMEs. A notable example of this is the use of AI in protecting against DDoS (Distributed Denial of Service) attacks, where algorithms can analyze traffic and block attempts to overwhelm servers before they are affected (Cisco 2022).

Another major benefit of AI in cybersecurity is the automation of incident response. In the event of a cyberattack, response time is crucial. AI algorithms can quickly analyze the nature of the attack, suggest countermeasures, and even initiate automated processes to isolate and mitigate the impact of the attack. This capability is particularly valuable for SMEs, which often lack sufficient resources to manually manage cyber incidents.

AI-based automation allows SMEs to respond to threats much more quickly and efficiently, reducing exposure time and the financial impact of an attack. SOAR (Security Orchestration, Automation, and Response) solutions utilize artificial intelligence to orchestrate and automate incident responses, enabling SMEs to manage threats with minimal resources.

Another important application of AI in cybersecurity is behaviour-based security, which focuses on monitoring and analyzing user and system behaviour. This method uses AI to identify unusual activities that may signal account compromise or a security breach. For example, an AI algorithm can detect if a user is accessing sensitive data at unusual hours or from unusual locations and can automatically block access or require additional authentication (IBM 2023).

These systems are essential for preventing insider threats, which are becoming increasingly common and difficult to detect using traditional methods. AI provides SMEs with additional protection by analyzing all network activities in real-time and identifying potential internal threats (Trend Micro 2023).
Artificial intelligence plays a crucial role in enhancing cybersecurity for SMEs by offering advanced solutions for the detection, prevention, and automated response to cyber threats. Machine learning algorithms and predictive AI provide SMEs with stronger protection against sophisticated attacks, while automated solutions reduce the need for manual intervention, saving time and resources. In an increasingly complex digital landscape, implementing AI is a critical step for SMEs in developing an effective cybersecurity strategy.

In the context of cybersecurity, decentralized threat intelligence sharing has become an essential component for preventing and combating cyberattacks. This practice involves the exchange of data and information related to cyber threats between organizations, platforms, and communities in a decentralized manner, without a single centralized entity managing these exchanges. Decentralized sharing offers SMEs a unique opportunity to collaborate globally and access essential information about emerging threats without having to invest significant resources in developing their own solutions (ENISA 2023b).

Decentralized threat-sharing platforms are key tools that enable organizations, including SMEs, to collaborate and share threat data efficiently. Examples of such platforms include MISP (Malware Information Sharing Platform) and STIX/TAXII (Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information), which facilitate the automated exchange of information about indicators of compromise (IOC) and tactics used by attackers (MISP Project 2023).

These platforms allow SMEs to stay informed about the latest threats without having to rely on costly commercial solutions. Participating organizations can share information about attacks, vulnerabilities, and abnormal behaviours in a

standardized and secure manner. This data exchange improves SMEs' ability to quickly identify and respond to cyber threats, especially zero-day attacks, which are difficult to detect using traditional solutions (OWASP 2023b).

One of the main advantages of decentralized threat intelligence sharing is the elimination of dependence on a single centralized entity to manage the flow of data. This increases the resilience of information-sharing networks and reduces the risk that a security breach in a centralized entity could compromise the entire system. Additionally, decentralization allows for faster and more efficient data exchange, as organizations can share information directly with each other without waiting for validation or management by a central entity.

For SMEs, decentralization represents an accessible and flexible solution, allowing them to access critical threat data in real-time without significant additional costs. For example, through decentralized sharing, SMEs can collaborate with other organizations in the same industry to protect themselves against targeted attacks, such as ransomware attacks affecting supply chains.
Decentralized threat intelligence sharing is complemented by the use of artificial intelligence (AI) to quickly analyze and interpret the data received. AI algorithms can process large volumes of data shared on decentralized platforms and identify patterns that would be difficult to spot manually. This capability enables faster detection of attacks and coordinated cyber campaigns.
For instance, machine learning algorithms can correlate threat data from various sources and alert SMEs to attacks that are rapidly spreading across multiple regions or industries. In addition, AI can help classify and prioritize threats, allowing SMEs to focus their limited resources on the most relevant risks.

Although decentralized threat intelligence sharing brings numerous benefits, there are concerns about the security and confidentiality of the shared data. SMEs need to ensure that sensitive information about their own infrastructure or experienced attacks is not exposed without authorization. For this reason, information-sharing platforms use advanced encryption and authentication methods to protect the confidentiality of the data (Cisco 2023).
For example, TAXII (Trusted Automated eXchange of Indicator Information) uses secure communication channels to ensure that only authorized organizations can access and share threat information. Moreover, many platforms allow data anonymization, giving SMEs the option to share indicators of compromise without revealing specific details about their own networks.

Another important aspect of decentralized sharing is international collaboration. Cyberattacks are often coordinated globally, and decentralized threat intelligence sharing allows SMEs to collaborate with organizations from other countries to combat these attacks. International cybersecurity organizations, such as FIRST (Forum of Incident Response and Security Teams), facilitate data sharing between

countries and economic sectors, contributing to a more effective global defence against cyber threats (FIRST 2023).
Decentralized threat intelligence sharing is an essential strategy for SMEs, allowing them to quickly access emerging threat data and collaborate globally to improve cybersecurity protection. By combining these platforms with artificial intelligence, SMEs can more effectively detect and prevent cyberattacks. However, it is crucial for SMEs to adopt proper security and privacy measures to protect sensitive information shared through these platforms.

This study is based on a detailed and multidimensional analysis of open-source solutions for the cybersecurity of small and medium-sized enterprises (SMEs), highlighting not only their effectiveness but also their practical applicability in the economic and technological environment of Romania. This section is dedicated to interpreting the data obtained during the research and emphasizes the specific contribution of the authors in developing the presented conclusions.

The analyzed data revealed a clear trend of increasing adoption of open-source solutions by SMEs. The included case studies, such as the implementation of PfSense in an IT-sector SME, demonstrated that these technologies can significantly reduce the number of successful attacks (by up to 80%) and generate cost savings of up to 70% compared to commercial solutions. These figures underscore the fact that SMEs can achieve a high level of security without making major financial investments.

The analysis highlighted the essential role of initiatives such as HackOlympics and decentralized information-sharing platforms. These collaborative frameworks provide SMEs with access to global resources and technical expertise, enabling them to adopt validated solutions and respond more effectively to cyber threats. Specifically, the collected data showed that SMEs involved in such initiatives reported a 50% improvement in their ability to detect and respond to complex attacks.
International standards, such as ISO/IEC 27001, were identified as essential for building a robust security system. Comparatively, SMEs that adopted these standards demonstrated a significant reduction in operational vulnerabilities and gained the trust of clients and partners.

The authors contributed an integrated analysis that adapted open-source solutions to the specific needs of Romanian SMEs. Case studies were carefully selected and documented to provide concrete examples of implementation, illustrating both the benefits and limitations of these solutions. For instance, the implementation of PfSense was detailed to demonstrate not only the reduced costs but also the steps necessary for configuring a customized firewall.

The authors emphasized the relevance of global initiatives for Romanian SMEs, tailoring the conclusions to the local context. By including HackOlympics and platforms such as MISP and STIX/TAXII, the study highlighted how SMEs can

benefit from international collaboration without requiring additional financial resources.
The authors developed a methodological approach that can be replicated by other SMEs, offering a practical guide for integrating open-source solutions and international collaboration. This model is based on a comparative evaluation of available solutions and clear recommendations for their gradual implementation.

The authors' contribution is also reflected in promoting a paradigm shift in how SMEs perceive cybersecurity. By including educational strategies and highlighting the benefits of collaboration, the study aims to transform cybersecurity from a challenge into a strategic opportunity for SMEs.
The interpretation of the data and observations in this study confirm that open-source solutions and international collaboration are essential pillars for strengthening the cybersecurity resilience of SMEs. The authors' personal contribution lies in the applied analysis and the integration of global perspectives into the local context, providing SMEs with a valuable and pragmatic guide to navigating the current cybersecurity landscape. This study not only offers solutions but also inspires a mindset shift, encouraging SMEs to adopt a proactive and collaborative approach to addressing digital challenges.

Conclusions

In the era of rapid digitalization, cybersecurity has become a central challenge for all organizations; however, SMEs are particularly vulnerable due to limited resources. This study has demonstrated that open-source solutions and international collaboration are essential keys to strengthening the cybersecurity resilience of SMEs, providing them access to advanced technologies and a global support ecosystem.

Open-source solutions have proven to be a strategic, accessible, and efficient resource for SMEs. In an environment where commercial solutions are often financially out of reach for small and medium-sized enterprises, open-source solutions offer not only affordability but also flexibility. SMEs can implement solutions tailored to their specific needs, enabling them to secure their digital infrastructures without incurring prohibitive costs. Additionally, the transparency of the code and the support of the global community enhance security by enabling the rapid identification and remediation of vulnerabilities.
International collaboration, supported by initiatives such as HackOlympics, creates a framework for collaborative learning and continuous testing of security solutions. This approach allows SMEs to benefit from validated solutions in a competitive environment and to learn from the experiences of other companies and cybersecurity specialists. The sharing of threat information through decentralized data exchange facilitates SMEs' access to critical information about attacks and vulnerabilities, contributing to faster and more efficient responses to risks.

Artificial intelligence has become an indispensable tool in detecting and preventing cyberattacks. Machine learning algorithms enable real-time identification of abnormal behaviours and emerging threats, providing SMEs with enhanced protection against sophisticated attacks. Automating incident response reduces reaction times and minimizes the impact of attacks, allowing SMEs to manage their limited resources more effectively.

Although open-source solutions and artificial intelligence offer significant opportunities, SMEs must be aware of the challenges associated with their implementation. The lack of technical resources and the need for expertise to properly configure and manage these solutions are obstacles. Furthermore, decentralized sharing of threat information requires rigorous security measures to protect data confidentiality. To maximize the benefits, SMEs must invest in employee education and training, as well as in adopting best security practices.

Open-source solutions, international collaboration, and the use of artificial intelligence provide SMEs with remarkable opportunities to enhance their cybersecurity. These strategies enable SMEs to effectively address today's digital challenges and strengthen their resilience against future cyber threats. The adaptability and accessibility of the solutions analyzed in this study can transform SMEs into more secure and robust actors within an increasingly complex cyber environment.

The present study demonstrated, with remarkable clarity, that small and medium-sized enterprises (SMEs) can overcome specific cybersecurity challenges by adopting a well-defined set of open-source solutions and actively participating in international collaboration initiatives. In a digitalized era where the complexity of threats is growing exponentially, this research outlines a concrete path for SMEs, enabling them to turn constraints into opportunities and strengthen their cybersecurity resilience.

From the outset, the study established three main objectives: a) Identifying accessible and efficient solutions for SMEs: The analysis demonstrated that open-source technologies such as PfSense, Suricata, and OpenVAS provide SMEs with the necessary tools to implement customized security measures without incurring prohibitive costs. b) Exploring the framework of international collaboration: Through initiatives such as HackOlympics and decentralized sharing platforms, the study emphasizes that SMEs do not operate in isolation but are part of a global ecosystem capable of responding to threats in a coordinated manner. c) Promoting the adoption of integrated strategies: The study proposes a strategic vision combining technological solutions, international collaboration, and compliance with global standards such as ISO/IEC 27001 to support SMEs in building a secure and scalable cyber environment.

The conclusions faithfully reflect these objectives, demonstrating that the analyzed solutions and strategies not only meet the immediate needs of SMEs but also provide them with a long-term competitive advantage.

This study's practical and detailed approach to a critical issue is a notable contribution. The authors successfully synthesized a significant volume of data and presented solutions adapted to the specific needs of SMEs in today's environment.
Through a comparative analysis of technologies like PfSense, Suricata, and OpenVAS, the authors highlighted not only the benefits of these solutions but also how they can be gradually integrated into IT infrastructures. The case study demonstrated their applicability in a real-world context, offering SMEs a scalable and replicable model.

The study anchored the challenges faced by Romanian SMEs within a broader European and international framework. Initiatives such as ENISA, HackOlympics, and decentralized sharing platforms were analyzed in detail, emphasizing the importance of international collaboration in creating a safe and sustainable ecosystem.
The authors emphasized the adoption of global standards such as ISO/IEC 27001, demonstrating that these norms are not merely bureaucratic requirements but opportunities to structure a robust security system and gain the trust of partners and clients.

The findings are relevant and immediate, providing SMEs with a strategic guide to confidently address cybersecurity challenges. By adopting the proposed solutions, SMEs can:

a) Reduce costs through free or low-cost open-source solutions;
b) Customize and expand the implemented solutions based on business growth;
c) Access resources, information, and technical support through international initiatives.

Additionally, this study underlines that SMEs can become proactive actors in cybersecurity, contributing to the global ecosystem by sharing threat information and adopting best practices.
This research paves the way for future investigations, including the long-term impact analysis of adopting open-source solutions in SMEs and evaluating new global initiatives supporting cybersecurity. By emphasizing the importance of collaboration and innovation, this study becomes a reference point for SME strategies in the digital era.

This study successfully integrates the technical, economic, and strategic aspects of cybersecurity into a holistic approach. By adopting the proposed solutions and actively participating in global initiatives, SMEs will not only improve their cybersecurity but also contribute to strengthening a safer and more collaborative digital environment globally. This is, in essence, the central contribution of this

research: transforming vulnerabilities into opportunities and SMEs into reliable partners in an increasingly interconnected digital economy.

References

Arbor Networks. 2023. DDoS Attacks: How Vulnerable Are SMEs? https://arbornetworks.com/ddos-attacks-smes.

Cisco. 2022. AI-Powered DDoS Prevention and Mitigation. https://cisco.com/ai-ddos-prevention.

—. 2023. Securing Decentralized Threat Intelligence Platforms. https://cisco.com/decentralized-threat-intelligence.

ENISA, European Union Agency for Cybersecurity. 2023a. Artificial Intelligence and Cybersecurity: Challenges and Opportunities. https://enisa.europa.eu/ai-and-cybersecurity.

—. 2023b. Threat Intelligence Sharing: A Key to Resilience. https://enisa.europa.eu/threat-intelligence-sharing.

—. 2023c. ENISA Threat Landscape Report. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

European Commission. 2023. Annual Report on European SMEs 2022/2023. https://single-market-economy.ec.europa.eu/document/download/b7d8f71f-4784-4537-8ecf-7f4b53d5fe24_en?filename=Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf.

FIRST, Forum of Incident Response and Security Teams. 2023. Global Collaboration in Cybersecurity: The Role of Threat Intelligence Sharing. https://first.org/global-cybersecurity-collaboration.

Gartner. 2023. Predictive Analytics in Cybersecurity for SMEs. https://gartner.com/predictive-cybersecurity-smes.

IBM. 2023. Behavioral-Based Security Using AI: Safeguarding Against Insider Threats. https://ibm.com/ai-behavioral-security.

MISP Project. 2023. Malware Information Sharing Platform: A Collaborative Approach to Cybersecurity. https://misp-project.org/malware-information-sharing.

NIST. 2022a. Cybersecurity Framework for Small and Medium Businesses. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

—. 2022b. Small Business Information Security: The Fundamentals. https://nist.gov/small-business-security.

OWASP, Open Web Application Security Project. 2023a. Open-Source Security Solutions for SMEs. https://owasp.org/open-source-security-smes.

—. 2023b. STIX/TAXII: Enabling Automated Threat Information Sharing for SMEs. https://owasp.org/stix-taxii-sharing.

PfSense Project. 2023. Firewall and Router Solutions for Small Businesses. https://pfsense.org/firewall-small-businesses.

Ponemon Institute. 2023. How AI is Transforming Cybersecurity for SMEs. https://ponemon.org/ai-transforming-cybersecurity.

SANS Institute. 2023. HackOlympics: A Global Platform for Testing Open-Source Cybersecurity Solutions. https://sans.org/hackolympics-cybersecurity.

Symantec. 2023. The Role of Predictive AI in Cybersecurity. https://symantec.com/predictive-ai-cybersecurity.

Trend Micro. 2023. AI and Insider Threat Detection in SMEs. https://trendmicro.com/ai-insider-threats.

Verizon. 2023. Data Breach Investigations Report. https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

FUNDING INFORMATION

Enhancing Security of European SMEs in Response to Cybersecurity Threats (SECUR-EU)", grant agreement no. 101128029, funded under DIGITAL-ECCC-2022-CYBER-03.

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

State of Siege in South Dobrogea. Action plan and instructions against attacks by Bulgarian komitadjis developed by the 9th Romanian Division command

Daniel Silviu NICULAE, Ph.D.*

*"Dimitrie Cantemir"Historical Association - A.S.I.C. Bucharest, Romania
e-mail: danielniculaie@yahoo.com

Abstract

On December 10, 1864, at the proposal of the ruler Alexandru Ioan Cuza, was voted by the Romanian parliamentarians, the Law on Siege, a basic normative act for future regulations in the field. The first article stated that the state of siege could only be declared in the event of imminent danger to public safety and order. In the context of domestic political events that took place in 1864, regulation of the agrarian problem and electoral rights, legislative initiatives that determined the coup of May 2, 1864, the phrase safety and public order unseen in the first article of the law, it was primarily aimed at ensuring the exercise of public authority in implementing the reforms undertaken by the government led by Mihail Kogalniceanu and implicitly protecting the population and the territory. Like an arch in time, in 1926, in peacetime, after 62 years since the vote on the Siege Law of 1864, the attacks of the Bulgarian comitages threatening the population, territory, and the exercise of state authority at the southern border imposed the extension of the provisions on the state of siege and their application by the War Council of the 9th Division.

Keywords:
South Dobrogea; state of siege; komitadjis; 9th Romanian Division; terrorism.

Article info
Received: 2 October 2024; Revised: 1 November 2024; Accepted: 13 December 2024; Available online: 17 January 2025

Citation: Niculae, D.S. 2024. "State of Siege in South Dobrogea. Action plan and instructions against attacks by Bulgarian komitadjis developed by the 9th Romanian Division command.." *Bulletin of "Carol I" National Defence University*, 13(4): 287-298. https://doi.org/10.53477/2284-9378-24-64

Considerations regarding the history of the siege state in South Dobrogea (Cadrilater) and the presence of border guards, gendarmes units, and 9th Romanian Division troops

On August 14, 1916, after 2 years of neutrality, Romania entered World War I after the signing of the Treaty of Alliance and the Military Convention with Entente. On the same day was published Royal Decree no.2798 for the declaration of the state of siege in the 34 counties of Romania in which the jurisdiction of the civil authority on the field of safety and public order was transferred to the military authority that was exercised by the ministry of war, army or division corps and prefects of counties who were militarized and assimilated to the ranks of the military hierarchy. All crimes committed against state security were tried by military courts. On June 30, 1918, the Royal Decree no.1626 was issued, which provided for the continuation of the state of siege on the territory of Romania, implicitly in South Dobrogea (Cadrilater) and Old Dobrogea, was issued, territories occupied by the troops of the Central Powers, from 1 July 1918, under the direct coordination of the military authority.

This was the legal framework at the time of the signing of the Thessaloniki Armistice on 29 September 1918 between Bulgaria and the Allied Powers, following requests made by the Bulgarian government on 24 September 1918, whose effect was the immediate cessation of all Bulgarian military operations. According to the articles of this document, in addition to leaving the German and Austro-Hungarian troops within 4 weeks of the Bulgarian territory, allied forces had the right to temporarily occupy certain strategic points and move and station within Bulgaria, with the mission to ensure compliance with the armistice clauses and to ensure peace and public order, but this last goal was very difficult to achieve, which is why, The Interallied Command in Sofia expressly requested support from the Romanian troops, which, according to the provisions of the Royal Decree no.1626/June 30, 1918, had the obligation to maintain public order on the Romanian territory of which both the South Dobrogea (Cadrilater) was part, territory incorporated into the Romanian state on 10 August 1913 by the signing of the Treaty of Bucharest and Old Dobrogea, a province united with Romania under the Treaty of Berlin of 1878. It should be noted that the two mentioned provinces were occupied and administered by the Central Powers troops following the signing by Romania of the Peace (Treaty) in Bucharest on April 7, 1918, an act that was not promulgated by King Ferdinand I of Romania.

In this legislative context, the presence of the Romanian troops in the two provinces could generate a state of conflict in a period in which it was intended to settle any dissensions for the preparation of peace, which is why, the first armed troops reported in the two Romanian provinces were the detachments of gendarmes who joined the civil and ecclesiastical authorities.
In April 1919, General Henri Mathias Berthelot, the commander of the Danube Army, ordered the 5th Army Corps jurisdiction over South Dobrogea and Old

Dobrogea. According to the received provisions, the 5th Army Corps had the order to enforce the provisions of the Law on the state of siege, which was why 3 border guard companies were sent to South Dobrogea (Cadrilater), ordered in Silistra, Bazargic, and Turtucaia. Against the background of the withdrawal of French troops from South Dobrogea, the attacks and plundering of Bulgarian komitadjis on the Romanian population intensified, with the need for additional forces. In the first days of December 1919, the presence of the 2nd Battalion of the 23rd Romanian Infantry Regiment was reported in Silistra and the Bazargic forces of a battalion of the 33rd Romanian Infantry Regiment were reported. At the same time, gradually, the units of the 9th Romanian Division, such as those of the 35th Romanian Infantry Regiment, the 36th Romanian Infantry Regiment, and the 40th Romanian Infantry Regiment received plans for transport in the peace garrisons they occupied in 1920.

Tactically, the troops of the 9th Division occupied the area to the right of the Danube River, situated southwest between the border from Bulgaria, east of the Black Sea, and north of the old border of Dobrogea and the Danube. The mission of the division was to defend the border of South Dobrogea against the aggressions of gangs or armed detachments, to cover the mobilization and concentration of the 5th Army Corps in order to prevent an organized attack with strong means, preventing Bulgarian propaganda and the penetration of propaganda agents and maintaining public order (Romanian National Military Archives, General Staff Fund, 429).
The troops of the 9th Division carried out patrol missions behind the border to break any type of connection between Bulgarians on both sides of the border and to intervene in support of the Romanian border guards when the operative situation imposed it (Romanian National Military Archives, General Staff Fund, 397).

On 14 January 1920, it was published in „Monitorul Oficial" no. 212, Royal Decree no. 113/13 January 1920 ordering the suspension of the state of siege, the censorship of the press and any other publications in the old kingdom except Dobrogea (Romanian National Military Archives, Grand Staff Fund, 136). Shortly after, in March 1920, the 5th Army Corps specified by „Order no.1 regarding the maintenance of the state of siege in Dobrogea", as within 10 days of its publication, all those who would have weapons and for whom they did not have the special permit to carry weapons issued by the army corps, to hand them over to the urban communes at the Garrison Command, and in the rural ones at the gendarmes' stations that released receipts from a specific notebook drawn up for each weapon. At the same time, he ordered the search of the inhabitants and the gathering of weapons from those who, after the fulfilment of the term stipulated by the ordinance, asked for a permit for carrying a gun (Romanian National Military Archives, the Grand Staff Fund, 135)

On 31 March 1921 it was published in the Official Gazette no. 286, the Royal Decree no. 853/March 14, 1921, which provided for the application of the state of siege on the 30 km area, with the possibility of extending up to 50 km along the borders of the country from the junction point of the border of Yugoslavia with the

Hungarian border to the White Fortress, following the Hungarian, Czechoslovak, Polish, Russian border, then the border of the South Dobrogea (Cadrilater), being the establishment of new military areas administered by the military authorities (Pantelimonescu 1939, 39).

On May 17, 1922, it was published in the Official Gazette no. 33, Royal Decree no. 2162 whereby the state of siege in the South Dobrogea (Cadrilater) was reduced to an area of 15 kilometres bounded by an imaginary line south of Turtucaia, Bazargic and Balchik along the border with Bulgaria (Pantelimonescu 1939, 41).

On 24 August 1926, the Council of Ministers Journal no. 2807 of 24 August 1926 was issued, referring to the extension of the state of siege in the South Dobrogea (Cadrilater), according to which the crimes committed on the demarcation line of the area between the towns of Carvan – Cavarna were tried by the War Council of the 9th Division. Therefore, on September 9, 1926, the division commander issued Ordinance no.1, which stipulated the offences and offences that were part of the military authority according to the articles of the Criminal Code, Law on the organization of South Dobrogea and the Law on the suppression of new crimes against public silence. In order to fulfil the mission received, the division command developed the action plan for fighting the Bulgarian comitagies, dissidence and nationalization of the South Dobrogea (Cadrilater) for 1926.

Instructions and Action Plan for guarding the border of Dobrogea against attacks of komitadjis

According to these instructions, the troops of the border guards, the gendarmes, and those of the 9th Division had as mission the surveillance and guarding of the Dobrogea border against the attacks of the komitadjis under the direct coordination of the 9th Division command. The action plan provided for two assumptions and implicitly two border guard devices depending on the magnitude of the events that could take place. The first phase provided for the execution of customs guard missions against komitadjis and the second phase, for, the possibility of confronting strong and well-organized attacks of Bulgarian komitadjis in the context of bilateral political tensions (Romanian National Military Archives, General Staff Fund, 137).

For the first hypothesis or phase, the security measures provided for the situation in which the border guards needed support, with units from the Bazargic and Silistra infantry regiments being provided for intervention. These forces were constantly in a state of alert to be able to respond to a request within 6 hours (Romanian National Military Archives, General Staff Fund).

For the second hypothesis, phase or device, numerous and well-organized attacks of Bulgarian komitadjis, the action plan provided for the establishment of strong detachments made up of 2 or 3 weapons in order to be able to capture or reject

over the border the komitadjis gangs that managed to penetrate the Romanian territory detachments shall be made according to the action plan drawn up by the commander of the respective division. The transition to device no. 2 was ordered by the Ministry of War, the General Staff, and the Commander of the 2nd Army Corps which, however, was allowed to switch to this device and on its own initiative of the local command when the situation imposed it, in which case the measures ordered to the General Staff were immediately reported (Romanian National Military Archives, The Grand Staff Fund).

In order to carry out the action plan in good condition, the troops of border guards and gendarmes were operatively subordinated to the command of the areas according to the provisions of the 9th Division Command, which obligation to specify in the action plan to be imposed based on events, mission, sector of each unit, the means made available and the directives for subordinated units and training exercises. Based on this plan, the subordinated units also drew up a detailed action plan in the various assumptions. For urgent cases and so that the intervention of the troops from the front line, the ones in the state of alarm deployed near the border, is not late, it could be intervened at the direct request of the border guards with the express order that this type of situation be immediately reported to the higher authorities. For good communication, telephone connections were made between the various cover forces and the commandments (Romanian National Military Archives, General Staff Fund).

The border guards' troops through the border guard provisions had the mission to stop individual crossings or small groups of komitadjis. In case groups/bands of komitadjis were difficult to capture, the border guards asked for support from the Silistra and Bazargic alarm battalions, during which time the two groups of forces assembled were carrying out the orders of the Alarm Battalion Command, which appreciated the situation and had the means and plan of action to capture, destroy or reject the komitadjis gangs. As long as the gangs were not made up of regular troops, their goal was to spread panic, loot, and propaganda, therefore, it is recommended to participate in the attack of limited forces in order to attract komitadjis in certain directions from where the thick of the detachment can more easily manoeuvre and capture them by enveloping. The opening of fire from great distances was not recommended because, besides alerting komitadjis about the presence of Romanian troops, it allowed them to change direction. If the komitadjis were heading to a locality, the instructions provided for the occupation of the liziers and the barricade near them with few forces, in order to allow the thick of the detachment to envelop the flanks and capture them. If the komitadjis managed to enter a locality, it is recommended to control the exits with a minimum of armed forces with automatic weapons to allow the bulk of the troops to capture them (Romanian National Military Archives, The Grand Staff Fund).

Concerning the collection and processing of information, the instructions provided for the organization of the intelligence service by the 9th Division Command to

be able to move easily and effectively to the execution of the action plan and the transition from one device to another depending on the situation that was imposed. The execution of the action plans also depended on the readiness of the commanders and the forces involved, for which reason, the units that guarded the Dobrogea border needed to become familiar with the land and the manoeuvres that were to be executed in concrete cases. In the composition of the action plan, the support that the civilian population could give where it can certainly count on its loyalty was also envisaged. Based on these instructions, the 9th Division Command drew up an action plan that was approved by the 2nd Army Corps, a copy being submitted to the General Staff (Romanian National Military Archives, The Grand Staff Fund).

According to this Action Plan, komitadji was defined as the one who carried a gun and used it. The one who was disarmed or the one who submitted to the summons had the right to legal treatment and protection. For the execution of the plan, the division command did not intend to act in the siege area under the conditions of military occupation or military dictatorships that would remove the civil administration and prevent the smooth running of social and economic relations, on the contrary, desiring the most discreet presence of the military forces as possible, he proposed an open and sincere collaboration with the administrative civil institutions, because they together with the gendarmes, border guards, and the loyal population, to develop an effective defence and reaction system against the attacks and incursions of Bulgarian komitadjis in the Romanian territory (Romanian National Military Archives, Grand Staff Fund).

Therefore, the Action Plan provided, in addition to warning that excesses of zeal were not tolerated and recommended to apply it with severity but with justice and legality, against komitadjis attacks a fixed and mobile defence, and against Bulgarian dissidence, the organization, and operation of a select intelligence and counterintelligence service. The fixed defence envisaged a border/guard zone prohibition zone, an organized resistance system/villages/endowed with a fixed and mobile garrison, and, a complex system of observations and information and a sophisticated system of links and transmissions. The mobile defence consisted of footbridges and horseback riding (Romanian National Military Archives, Grand Staff Fund).

According to the Action Plan, the perimeter of the state of siege was divided into the operative area under strict military command, where the border guards whose record was komitadjis death and the arrest of criminals, and the cooperative area, acted, under mixed command, in which all the institutions involved in the defence strategy had the mission of ensuring public order (Romanian National Military Archives, General Staff Fund).

In the operative area of the border guards, the device of the troops was positioned in depth about 8-10 kilometres with 4 echelons, with a considerable density in

vulnerable regions and previously confirmed observers and border guards, indoor battle stations, subsector reserves, mobile units/cavalry/support and control. In the amplitude of the sectors, it was minimal and variable depending on the configuration of the land, and in Caliacra it was directly proportional to the regions where the komitadjis were acting. The repainted forces in this area consisted of 3 border guards, 23 infantry groups, 12 infantry platoons, 2 red squadrons and 2 telegraph sections. The mission received by these troops had 3 dimensions, namely military – territory security, fiscal - according to the instructions of the Ministry of Finance, and technical and administrative - according to the orders and directives of the Border Guard Corps. In order to better carry out the missions received, the commander of the guard battalion had to draw up the plan of organizing the command, of the connections and transmissions, of the information and observations, of the mission and the record as well as the reports and reports (Romanian National Military Archives, Grand Staff Fund).

Regarding the cooperative zone, the gendarmes and administration area or the internal defence system, the Action Plan had special measures such as knowledge of village psychology, their administrative-military organization, nominal identification/identity cards with photos of the male part, classification of the population of the villages into reliable, doubtful or bad locals. The former were treated as allies, the wicked in pursuit and the others were kept under observation by the gendarmes who had to understand a good knowledge of the villages was a point won against the komitadjis. It was known by the 9th Division command that Bulgarian villages were for intelligence and espionage offices, supply centres and hosting sites. Therefore, the gendarmes had to take measures on interception of links; prohibition of supply and exclusion of the possibility of hosting. In order to achieve these objectives, the administrative authority of the localities entering the siege zone was preserved, and groups of villages/relating to distances, number of inhabitants, geographical situation and spirit of population were organized. Each group of villages had a military commander and each had a joint command/military and the respective praetor. Each locality had a force made up of gendarmes - effectively between 5-7 people, a citizen guard/relating to the number of villages/ alarm units and night caroules with the mission to defend the respective localities. The mobile formation, whose number was a maximum of 5 riders, was formed daily from the fixed garrison and had village horses/made available by the commune. The mission of this mobile force was to research the space between villages and the ways of communication. The core of the garrison is ad hoc represented by the rural gendarmes' patrols or horsemen, and the village group command had a small garrison/gendarmes and citizens on horseback and foot, and the Plaza Commands had a reserve of rural gendarmes, an information service and a service to supply units residing on the territory of the plate (Romanian National Military Archives, The Grand Staff Fund).

Regarding the division of the siege area into sectors that were the responsibility of the regiments of the 9th Division, the Action Plan included 2 sectors, namely the

Mircea Sector, where the 38th Romanian Infantry Regiment and the Vlad Sector were operating, the 40th Romanian Infantry Regiment. The mixed command of the sectors is exercised in depth by the regiment commanders in close cooperation with prefects. The 9th Division went into cover with 16 platoons from the 38th Romanian Infantry Regiment and the 40th Romanian Infantry Regiment (8 each regiment). The herds of a platoon, only from the 1925 contingent, selected and perfectly framed, had a commander with 2 helpers, 25 troop soldiers of which 18 were combatants and 7 for patrols, observers and information. The armament consisted of 1 machine gun, 2 machine guns with servants, the rifles from the endowment of the 10 riflemen and the ammunition provided 10 grenades, 5 missiles, 100 weapon cartridges, 500 machine guns, and 250 Machine guns (Romanian National Military Archives, Grand Staff Fund).

As regards the means of communication and liaison, the Action Plan provided for one truck and telegraph station per sector. The trucks were distributed for the service use of the sector commanders and the transport of operative troops. On request and under certain conditions they were put into use by the commander of the guard battalion in the sector of each regiment (Romanian National Military Archives, Grand Staff Fund).

On detached posts and patrols at points too isolated and configurations too wild or wooded, it was stipulated that those in the border guard's area were decided by the commander of the border battalion in the interior area by the commanders of the sectors in collaboration and according to the indications of the mixed platbands. The patrols were ordered by the local chiefs, each in his command, by field, circumstances and daily information (Romanian National Military Archives, Grand Staff Fund).

The intelligence service consisting of observers and informers was organized in each sector, subsector, district grouping, unit and weapon and was run exclusively by the respective command after a well-thought-out plan. In the border guard's area were organized 4 centres and an office, established by the commander of the battalion of border guards. In the inner area, there were centres for each net. In the cavalry area – the centre for each squadron. To the sectors of the regiment – existing information offices. As regards reporting and reporting hours, it was stipulated that in sectors and subsectors, it should be carried out according to the provisions of the respective heads, with Division 9 from sectors by phone every day at 18 o'clock, newsletters, reports or reports every Sunday with weekly events; for urgent cases and by any means (Romanian National Military Archives, Grand Staff Fund).

As regards the supply of the troops, it was envisaged that it would be done with respect for the rights of the person and of the person, and the military units were not allowed to appeal to the local resources in the event of impossibilities of securing raw materials by direct source. It was expressly stipulated, under severe sanctions,

that for no reason was the personal supply or supply of the band directly from the inhabitants, but only through the local administration. Payment was made by the administration by issuing – vouchers signed exclusively by the commanders of the units, whose name was communicated in advance to the prefectures. The receipts were paid every 15 or 30 days with the legal forms certified by the administrative authorities. The commanders of the units sent advance Payment Reministration tables of monthly necessities with the indication of the lifting days. The border guards were supplied according to the administrative provisions of the Corps but remained under the same sanctions if they committed violations of rights or violated the administrative provisions of the Command (Romanian National Military Archives, General Staff Fund).

The action plan also had final provisions requiring detainees to be accompanied by a protective detachment. If there were more arrested, they were tied to each other and if the detainees tried to flee, it was forbidden to fire on them if they were not tried and convicted.

Although the action plan looked perfect on paper, in the field the reality was different. Romanian border guards and authorities were attacked by komitadjis, with daily reports of looting, robberies, injuries or killing of Romanian soldiers and gendarmes. However, the conception of the commander of the 9th Division, General Ioan Vladescu, regarding the rejection of the terrorist attacks of the Bulgarian komitadjis, was revolutionary, given that the military doctrine of 1926 did not provide for characteristic measures against asymmetric actions.

Conclusion

The establishment of a state of siege in South Dobrogea in 1926 was an exceptional measure ordered as a result of the attacks of Bulgarian komitadjis threatening the safety of the Romanian state. Against the background of the revisionist policy of the Bulgarian government which maintained a tense state on the border with Romania by supporting terrorist actions of komitadjis, political and military decision-makers in Bucharest, Romania, loyal to the principles of the Treaties concluded at the end of World War I, they managed the conflicting state on the southern border in a less addressed manner in the historiography of asymmetric conflicts. By investing military authority and by ordering measures, the commanders of the units arranged in the residence garrisons of South Dobrogea (Cadrilater), wrote a less-known page of military history. This article is a tribute to the gendarmes, the infantry troops and the Romanian civil authorities who contributed to promoting the values of the European principles assumed by Romania in the XX century.

References

Annals of Dobrogea. 2005. New series, year VIII, Constanța.

__. 2019. Series III, year III, Constanța.

Assan, B. G. 1912. *The Dobrogean Quadrilater, Rusciuc, Varna, Sumla, Silistra.* Bucharest: Minerva Publishing House.

Bulletin of the Romanian Military Archives. Year XX. Document. no. 3/2017.

Ciorbea, Valentin. 2008. *Dobrogea 1878-2008. Horizons opened by the European mandate*. Constanța: Ex Ponto Publishing House.

Filotti Alexander Gabriel. 2007. *Borders of Romanians.* vol. I and vol. 2. Brăila: Istros Publishing House of Brăilei Museum.

Ghițescu, Mihai. 2021. "About the state of siege in Romania, Historical-legal outline, 1918-1938." *Romanian Academy Library Review* Year 6, no. 12, July-December.

Cătălin Negoiță. 2009. Between Left and Right. Communism, irredentism and legionaryism in Quadrilater (1913-1940), Publisher of the Scrisul Românesc Foundation, Craiova.

King Ferdinand I National Military Museum. 2020. ***Tradition, History, Army.*** Fifth Edition, October 29, 2019. Târgoviște: Cetatea de Scaun Publishing House.

Kurkina Ana–Teodora. 2013. *The problem of the appurtenance of Dobruja region, 1913-1940: Bulgarian and Romanian methods of claiming rights over territory*. Budapest, Hungary: Central European University, History Department.

Neagoe Sever. 1985. *Territory and Borders in Romanian History*. Bucharest: Publishing House of the Ministry of the Interior.

Pantelimonescu, V. 1939. State of siege, Doctrine, Jurisprudence and Legislation, Bucharest, Universul Newspaper Publishing House.

Roman, Ioan N. 1905. *Dobrogea and the political rights of its inhabitants*. Constanța: Ovidiu Publishing House.

__. 2008. *About Dobrogea and Dobrogeni.* Constanța: Ex Ponto Publishing House.

Romanian Brotherhood newspaper. 1926. Year II, no. 23-24, October 1-15.

Romanian National Military Archives. Great Staff Fund.

The Greek, Gr.,D. 1928. *The current state of siege.* Bucharest: Curierul Judiciar S.A. Publishing House.

Ungureanu George. 2009. *The problem of the Quadrilateral in the context of Romanian-Bulgarian relations (1919-1940)*. Brăila: Istros Publishing House of the Brăilei Museum.


AGENȚIA ROMÂNĂ DE ASIGURARE A CALITĂȚII ÎN ÎNVĂȚĂMÂNTUL SUPERIOR
ROMANIAN AGENCY FOR QUALITY ASSURANCE IN HIGHER EDUCATION
Membră ENQA – Full member of ENQA
Înregistrată în EQAR – Registered in EQAR

CERTIFICAT
CERTIFICATE

Universitatea Națională de Apărare „Carol I" din București

a obținut, în urma evaluării instituționale, calificativul
GRAD DE ÎNCREDERE RIDICAT
pentru perioada 2021-2026
following institutional evaluation, attained the HIGH DEGREE OF CONFIDENCE rating for the period 2021-2026

BIROUL EXECUTIV AL CONSILIULUI ARACIS

EDITOR
„Carol I" National Defence University Publishing House
(Publishing house with recognized prestige validated
by the National Council for Attestation of University
Degrees, Diplomas and Certificates)
Adress: Panduri Street, no. 68-72, Bucharest, 5th District
e-mail: buletinul@unap.ro
Phone: +4021.319.48.80 / 0365; 0453

Signature for the press: 17.01.2025
The publication consists of 298 pages.