Legal and ethical aspects of the synchronization of military and non-military activities in multi-domain operations

Luiza SÎRBU (RADUSLAV), Ph.D. Student*

* "Carol I" National Defence University
e-mail: sirbu.luiza@yahoo.com

Abstract

The evolution of war and armed conflicts in contemporary society and in the foreseeable future requires deep reflection not only on the physiognomy of the confrontation but also on rethinking the ways of adapting the forms and procedures of military action to the requirements of international law, principles, and norms concerning the protection of victims, different categories of persons, and material and cultural assets. "Multi-domain operations" have a considerably increased potential for generating combined destructive effects achieved with means of combat based on new technologies. By synchronizing military and non-military activities, this mixing can, in turn, generate consequences that may fall under the law of armed conflict. In this context, our aim in this material is to identify some aspects that reflect the need to synchronize multi-domain operations with the legal regulations and ethical conditions necessary for conducting contemporary military conflicts.

Keywords:
war; operation; multi-domain; law; legal; moral; synchronisation.

Armed conflict involves the use of violence, which generates endless suffering, loss of human life, and material damage. Large populations, including children, women, the elderly, and helpless persons, caught in conflicts, are forced to go through these tragedies. Military actions implemented with increasingly destructive means of combat often defy reason and rationality. The character of the conflict is always changing, propelled by cultural, military, and technological evolution. In the past 20-25 years, the pace of change has accelerated, largely due to the emergence of new technologies that transformed the way conflicts are conducted and the operating environment in which they take place. Against this backdrop of continuous change, international humanitarian law, the law of military conflicts, and military ethics during armed conflicts of various natures must be subject to increased scrutiny.

The hybrid component of the war waged by the Russian Federation in Ukraine expands the battlefield by exploiting multiple military and non-military domains and dimensions. Culture, information, economy, technology, and society as a whole have become battlegrounds in this context. The demonstrative hybrid warfare on the Ukrainian battlefield would pose a particular challenge to Europe and to the crisis management and defense of both NATO and the EU if waged against European countries.

Countering hybrid actors and activities requires a comprehensive and coordinated response across multiple domains and battlespaces, and multi-domain operations appear to offer a solution in such scenarios. Therefore, there is a need to synchronize multi-domain operations with legal regulations and ethical conditions necessary to be met during the conduct of contemporary military conflicts. Thus, multi-domain operations are seen as representing "*the orchestration of military activities, in all domains and environments, synchronized with non-military activities to enable the Alliance to deliver convergent effects at relevant speed*" (NATO Standardization Office 2022, 3) and having greater destructive potential than the combined use of the categories of armed forces, the issue of compliance with the norms of international law becomes imperative.

Moreover, engaging in confrontation with the adversary simultaneously in one or more of the operational domains identified in the NATO Allied Joint Doctrine, namely maritime, land, air, space and cyber, along with the integrated use of capabilities of military and non-military organizations, results in transformations not only in the character of the fight itself but also in the increased legal and moral responsibility of decision-making regarding the organization of a great diversity of connected activities. This includes those related to the protection of direct and indirect victims from the effects of combat, which, in our opinion, requires a multi-domain approach to operations from this perspective as well.

The need for legal and ethical synchronization of multi-domain operations

Today, in the third decade of the 21st century, the evolution of the security environment has undergone profound transformations in political, economic, technical-scientific, social, and knowledge terms under the impact of the globalization phenomenon. With this evolution, new forms of crises and armed conflicts have emerged, and new means of combat have appeared in the theaters of military operations, posing multiple legitimacy challenges from the perspective of public international law and in terms of the incidence of international humanitarian law.

Even if it contains the norms of behavior during armed conflicts, international law cannot represent a substitute for peace, but "*a bulwark of humanity in the face of bloody provocations, a unique testimony of reason and hope to master force and mercy in the face of murderous aberration*" (Uscoi and Oprea 1999, 5). The same observation is also valid for military ethics as a set of rules of conduct that must be respected during armed conflicts.

The issue of the legal and moral aspects of synchronizing military actions with non-military activities in multi-domain operations must be contextualized, in our opinion, primarily in the discussion regarding the obligation imposed on states by contemporary international law to settle differences between them exclusively by peaceful means "*We, the Peoples of the United Nations - stipulates the UN Charter -, determined to free future generations from the scourge of war which, twice in the course of a human life, has caused untold suffering... And for these purposes let us practice tolerance and live in peace with each other ... and to establish methods to ensure that armed force will be used only in the common interest …*" (Organizația Națiunilor Unite 1945, 1).

Even though the precision of weapons has been perfected, they are now widely used on civilian targets, war as a whole affecting an increasing number of people and material, cultural and spiritual goods, calling into question the present and future of its development. However, while vast changes are taking place in the way war is waged, its human dimension still remains fixed – war has ethical limits. As some military specialists have noted, "*Battle on several fronts represents an intrinsic ethical dilemma for the combatant's ability to apply combat power in accordance with the principles of Jus ad Bellum and Jus in Bello inherent in the law of war*" (Hedrick 2018). Therefore, as strategies and tactics evolve, it is imperative to consider the legal and ethical ramifications of their military use. In addition, armed conflicts, whether international or internal, are often accompanied by other anomic phenomena such as hunger, disease, migration, and environmental destruction. These issues are often discussed but little action is taken due to the absence of universally accepted international regulations and rules, which must be respected and enforced through effective sanctions directed against those who violate them.

Furthermore, a study by the Rand Corporation states that "*revisionist approaches to just war theory challenge the legal definition of combatants because new types of cross-domain operations do not take into account the ethical intentions of individuals who are parties to the conflict. In this sense, non-combatants may be exposed to harm if their actions support an 'unjust war'*" (Retter, et al. 2016, V). Cyber and autonomous systems have also been considered to present challenges to a number of principles underlying traditional moral and legal frameworks.

Cyber-attacks, the use of drones as strike weapons, armed robots, fully autonomous weapons, not to mention the resumption of the rhetoric of the possibility of using, under certain conditions, weapons of mass destruction, are military actions against which, at the time, there are no specific covering regulations in international law and therefore in most cases reference is made to texts with general coverage, most often to the Charter of the United Nations, art. 36 of Additional Protocol I to the Geneva Conventions of 1949 or other existing international regulations. Moreover, according to the concept of multi-domain battle "*cyber-attacks against national economic interests represent an attack on a state's sovereignty, thus justifying lethal retaliation*" (Hedrick 2018, 42). While legal justification may protect such actions, moral and ethical justification is much more ambiguous.

The difficulty of categorizing this type of actions from the perspective of international law also arises from the challenge of identifying the perpetrator due to regulations being based on the classic form of war, with physical operations in real space and areas of contact more or less closely. However, contemporary armed conflicts involve operations that heavily rely on actions where the identity of the aggressor, their location, and the true beneficiary of the effects are difficult or impossible to identify.

Moreover, taking advantage of the inadequacy of some provisions of the documents that criminalize the violation of the principles and norms of international law, including international humanitarian law, to the transformations produced in society and in the phenomenon of conflict, in all armed conflicts there have been and are taking place reprehensible acts and actions from a legal and moral point of view, for which one has rarely been called to account in front of justice, although theoretically "*the populations and belligerents remain under the protection and under the empire of international law, as they result from the established usages among civilized nations, the laws of humanity and the exigencies of public consciousness*" (A patra convenție de la Haga 1907, Preambul).

All these must find solutions in the near future, taking as an example the regulations in the field of cyber warfare contained in the Tallinn Manual on the International Law of Cyber Warfare, but many other forms of manifestation of political-military conflict await the finding of appropriate ways of relating them to the principles and specificities of international law, because "*emerging technologies such as artificial intelligence, hypersonic, machine learning, nanotechnology and robotics lead to*

a fundamental change in the character of warfare ... their impacts have the potential to revolutionize the battlefield unlike anything since the integration of machine guns, tanks, and aviation that began in the age of combined arms warfare" (Milley 2018, i). In response to the transformation of the character of war and the need for a comprehensive approach to the need for global peace and security, the multi-domain operation was developed, which is "*carried out during three phases of operation: competition, crisis and armed conflict*" (DefenceNews 2022).

At NATO level, as the definition presented above also showed, the concept is based on the orchestration of military activities in all fields and spaces of the operating environment, coordination with non-military activities, which allow the production of convergences with a relevant speed, the fields representing entities from the operational environment in which synergistic actions to confront the adversary are organized and executed. At the same time, it combines actions from the physical environment with those from the informational non-material space or that act on the human psyche.

While at the NATO level the concept of multi-domain operations is visualized as an evolution, a higher form of development, of joint operations, from the US perspective, multi-domain operations are not differentiated from joint operations, being considered as representing the "*combined use of joint military and non-military weapons and capabilities to create and exploit comparative advantages to defeat enemy forces and consolidate victory*" (US Department of the Army 2022, 1-2).

Some doctrinal elements of the concept of multi-domain operations appeared in 2017 under the name "Concept Version 1.0 for Multi-Domain Battle", renamed in 2018 "Multi-Domain Operations" and presented in Pamphlet 525- 3-2, *The US Army in Multi-Domain Operations 2028*. The concept was built "*on the basis of the US Army doctrine of the 1980s 'Air-Ground Battle', designed in response to the threat posed by the Soviet Army in the European theater*" (Leon 2021, 92) at that time.

At the level of the British military, in 2020 the concept of "multi-domain integration" is being discussed, seen as "posting military capabilities in line with other national instruments of power, allies and partners; configured to perceive, understand and prevent threats in optimal time, across all operational domains and levels of war" (UK Ministry of Defence 2020, 3). Later, in 2021, multi-domain integration is developed in the "integrated operation concept" (UK Ministry of Defence 2021) seen as a way to counter adversary strategies aimed "*to undermine cohesion, erode economic, political and social resilience and compete for strategic advantages in key regions of the world*" (UK Ministry of Defence 2021, 3).

In the specialized literature, there are authors who claim that the new conception regarding the organization of confrontation with the adversary is based on three fundamental principles: *the calibrated posting of forces obtained by combining their*

positioning with the ability to maneuver them at strategic distances; the existence of multi-domain force structures that have the necessary capacity, capability and resilience to operate in multiple domains in volatile situations; the convergence of effects achieved through the rapid and continuous integration of capabilities in all physical domains, as well as in the non-material electromagnetic, informational and psychic space (Milley 2018, 17-24) which, other authors claim, "*solves the problem of contested domains and Anti-Access/Aerial Denial (A2/AD) threats presented by Chinese and Russian operations during periods of conflict*" (Garn 2019, i).

The cultural, technological, and military attributes that shape multi-domain operations, the ethical dilemmas created by emerging technologies, including those caused by the implementation of disruptive technologies, and the operational implications and strategic military actions in dense urban environments are key areas to consider on the multi-domain battlefield.

This new paradigm of military operations requires rethinking the ways of synchronizing military and non-military actions. This involves identifying appropriate solutions to the kinetic and non-kinetic problems that may arise in each of the confrontation domains, while also achieving the operational military objectives aimed at the support, assurance, and multidimensional protection of the forces, civilian population, environment, cultural heritage assets, and various categories of persons who must benefit from appropriate treatment according to the principles and norms of international humanitarian law.

National efforts towards conceptualizing the regulation of multi-domain operations

Romania has aligned itself with the efforts of the states of the world undertaken in the legal field, both legislatively and institutionally, capitalizing on "*the humanitarian traditions of the Romanian people, in general, of the armed forces, in particular, as well as the experience accumulated by the responsible structures in this field, especially as a result of participating in various international missions*" (Guvernul României 2005, Preambul).

Responding in a specific manner to the wishes deriving from the concept of multi-domain operations about to be imposed within NATO, Romania's Military Strategy introduces the concept of the **Integrated Combined Force** operation on the basis of which "*the Armed Forces of Romania, in an expanded inter-institutional format, will carry out assigned missions and tasks*" (Ministerul Apărării Naționale 2021b, 26). Also, in the Defence White Paper, reference is made among the specific requirements for the Romanian Armed Forces to a "*performing decision-making process, effective command-control system and the development of multi-domain and multi-domain response capabilities*" (Ministerul Apărării Naționale 2021a, 32). However, as noted

by Romanian military specialists, "*the multi-domain operation refers, in addition, to the clearly defined conventional military aspects, to non-conventional aspects, which is, in fact, one of the reasons why it was distanced at the doctrinal and conceptual level by the joint operation*" (Cucinschi 2021, 144).

Multi-domain operations are conducted during three operational phases: competition, crisis and armed conflict. They address the challenge of competitors using layered capabilities at a distance to deter, requiring Romania and its partners and allies "*to use ground-based capabilities to eliminate or diminish threats from enemy intelligence, surveillance and reconnaissance networks*" (DefenceNews 2022).

At the level of the Romanian Armed Forces, as presented by Romanian military specialists, "*the development of the MDO concept is still in the phase of study and doctrinal deepening, to be implemented in the period 2026 - 2032, during the second stage of the Program for the transformation of the Romanian Armed Forces until in 2040 – the implementation of new technologies and the reorganization of the armed forces for multi-domain actions. Until the end of the first quarter of 2022, measures were taken at the level of the Ministry of National Defence for the participation of experts and scientific researchers in various activities organized in the field of multi-domain operations and some scientific events were organized and carried out for the doctrinal analysis of the need to realize such a concept*" (Ioniță 2022, 72). Therefore, unlike other countries, such as the USA or the United Kingdom of Great Britain, which have moved to the implementation phase of the concept, Romania shows a slower evolution, which is primarily due to the need to "*develop multi-domain and multi-domain capabilities of response*" (Ministerul Apărării Naționale 2021a, 32) that use advanced technologies such as "*those incorporated in several military applications, namely: intelligence, surveillance and research (ISR), logistics, cyber operations, command and control (C2), semi-autonomous vehicles and autonomous in totality and the provision of optimal multi-annual investments for research-development-innovation activities*" (Ioniță 2022, 43). Also, training and preparing for multi-domain operations is undoubtedly a challenge for the Romanian Armed Forces, especially trying to keep up with the developments of allies and partners, as well as potential adversaries. The reality is that it is incredibly difficult to bring together air, land, naval and space personnel and assets in a cyber-secure environment, even more so when it needs to be done quickly, consistently and cost-effectively.

Conclusions

The rules of war have changed, and with the emergence of hybrid conflicts, the role of non-military means in achieving political and strategic objectives has increased. In many cases, they have surpassed the power of weapons in their effectiveness. Thus, the focus in terms of combat methods applied in the conflict has also changed

towards the widespread use of economic, informational, humanitarian policies, and other non-military measures.

The concept of multi-domain operations has become dominant in military standards, defence discussions, concept papers, and opinion articles, as it is seen as the integrative and comprehensive solution for national and collective defense against hybrid threats. Multi-domain operations also create multiple legal and moral responsibilities stemming from the specificities of their application in the respective domains. Thus, it is necessary to better contextualize the principles and norms of the law of armed conflicts in relation to the new challenges of political-military conflict and the development of forms, methods, and mechanisms intended to repress the violation of these regulations.

Future conflicts will involve the use of all five combat domains (land, air, sea, space, and cyber). Therefore, it is increasingly important for the Romanian Armed Forces to continue developing and deploying new weapons and technologies that will ensure the successful completion of future national and allied missions. In short, the force structure must be transformed to meet future warfighting requirements.

References

A patra convenție de la Haga. 1907. "Convenția privind legile și obiceiurile războiului pe uscat." 18 oct. https://www.arduph.ro/files/articles/Conven%C8%9Bia%20(Regulamentul%20)%20referitoare%20la%20legile%20%C5%9Fi%20obiceiurile%20r%C4%83zboiului%20pe%20terestru,%20Haga,%2018%20octombrie%201907.pdf

Congressional Research Service. 2022. "Defense Primer: Army Multi-Domain Operations (MDO)." November 21.

Cucinschi, Alexandru-Lucian. 2021. „Impactul operației multi-domeniu asupra strategiei militare." *Gândirea Militară Românească* 144.

DefenceNews. 2022. *Multidomain operations concept will become doctrine this summer.* March 24. https://www.defensenews.com/land/2022/03/23/multidomain-operations-concept-will-become-doctrine-this-summer/.

Garn, Alex R. 2019. *Multi-Domain Operations: The Army's Future Operating Concept for Great Power Competition.* Fort Leavenworth, KS: US Army Command and General Staff College.

Guvernul României. 2005. *Strategia națională a României de aplicare a dreptului internațional umanitar.* București.

Hedrick, Bryan. 2018. "First to Fight for the "Right": The Ethical Dilemma Inherent Within the Multi-Domain Battle Concept." *Small Wars Journal.* https://smallwarsjournal.com/jrnl/art/first-fight-right-ethical-dilemma-inherent-within-multi-domain-battle-concept.

Ioniță, Crăișor-Constantin. 2022. *Societatea postindustrială și inteligența artificială. Provocări și oportunități din perspectiva securității naționale și a NATO privind dezvoltarea conceptului operație multidomeniu.* București: Editura Universității Naționale de Apărare „Carol I".

Leon, Jose Diaz de. 2021. "Understanding Multi-Domain Operations in NATO." *The Three Swords Magazine* (NATO Joint Warfare Centre) (37): 91.

Milley, Mark A. 2018. "The U.S. Army in Multi-Domain Operations 2028." *TRADOC Pamphlet 525-3-1* i. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

Ministerul Apărării Naționale. 2021a. *Carta Albă a Apărării.* București.

—. 2021b. "Strategia militară a României." București.

NATO Standardization Office. 2022. "AJP-01. Allied Joint Doctrine." Edition F, Version 1. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1128191/AJP-01_EdF_V1.pdf.

Organizația Națiunilor Unite. 1945. *Carta Națiunilor Unite.* San Francisco.

Retter, Lucia, Alex Hall, James Black, and Nathan Ryan. 2016. *The moral component of cross-domain conflict.* Cambridge: Rand Corporation.

UK Ministry of Defence. 2020. "Joint Concept Note 1/20 Multi Domain Integration." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf

—. 2021. "Integrated Operating Concept." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf

US Department of the Army. 2022. "FM 3.0. Operations." https://irp.fas.org/doddir/army/fm3-0.pdf

Uscoi, Nicolae and Gabriel Oprea. 1999. *Introducere în Dreptul Internațional Umanitar.* București: Editura Cartega.