

THE ROLE OF MULTI-DOMAIN OPERATIONS IN MODERN WARFARE

Ionela Cătălina MANOLACHE

Headquarters Multinational Division South-East Bucharest, Romania
catalinagrigore2694@yahoo.com

ABSTRACT

The end of the Cold War and the emergence of modern technologies, especially in the space or cyber fields, brought a new interpretation of conflicts, based on modern systems and decisions adapted to these novelties. It is through these considerations that the changing nature of conflicts has presented challenges to traditional military doctrines and strategies. The multi-domain operations approach is used by NATO to identify the unique strengths and capabilities of each force category. By identifying these capabilities, the Alliance is able to create plans that maximize the effectiveness of each force category and enable a more effective response to potential threats.

KEYWORDS: multi-domain, NATO, threat, conflict

1. Introduction

Human history cannot be understood if it is not associated with the conflicts and crises that have marked it. Most areas of society have been shaped or influenced by war. Over time, historians and military specialists have studied numerous documents to identify and highlight lessons and principles that can support the development of doctrines to underpin the next stages of evolution in the conduct of conflicts.

In a conflict or competitive context, deception is used to support a particular plan or strategy. The degree of success of the deception component will, most of the time, be directly proportional to the success of the plan.

Compared to the last century, the number of operations carried out by the armed forces is much higher today (NATO, 2023). Conflicts have become more complex, they are fought by state or non-state actors, and the importance of having the skills to execute misleading actions is

crucial. As a result, in the dynamics of most conflicts, the execution and detection of deception is an essential part of the actions carried out in the confrontational space.

Multi-domain operations (MDO) represent a new military concept, aimed at countering the challenges generated by emerging technologies and threats from state and non-state actors. This new approach recognizes the interdependence and interconnectivity of various domains of action, such as land, air, maritime, space, information or cyber, and seeks to integrate them.

If the doctrinal approach is not adequate, the possible military advantages available to the security organizations can be diminished. For example, the North Atlantic Treaty Organization (NATO) is forced to update its conceptual link between the foundations of human conflict and new developments that bring about important changes in the character of war. However, the aggression launched by Russia against Ukraine represents an important

opportunity for NATO to reevaluate some of its doctrinal aspects. The conflict highlighted the importance of cybernetic and space actions, the utility of unmanned systems, and the value of flexible-thinking commanders who can deliver effects across multiple domains, rapidly and at scale.

There are currently no documented works or manuals regarding misleading in multi-domain operations. Along the lines of misleading, both the Romanian Army, the US Army and NATO have a series of regulations in force. Along the lines of the specialized literature, the field began to consolidate.

The US Armed Forces were the first that began to draw certain directions along the lines of multi-domain operations through a series of works such as: *“The U.S. Army in Multi-Domain Operations 2028”* from 2018, *“U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade – 2025-2045”* from 2018, *“Army Multi-Domain Transformation – Ready to Win in Competition and Conflict”* from 2021 and also from the same year, *“The Army in Military Competition”*. The latest manual, *“F.M. 3-0 Operations”* launched in 2022 theoretically strengthens the multi-domain approach by the US Army. At the NATO level, in 2022 the AJP-01 manual appeared, which touches on aspects of approaching operations from a multi-domain point of view. At the level of the Romanian Army, there is still no manual covering multi-domain operations. However, there is interest in this approach and the Romanian textbooks will most likely be updated to cover the new approach.

The purpose of this article is to highlight the relevant aspects regarding the execution of the new models of operations – multi-domain operations, with an emphasis on identifying some command-and-control trends regarding this concept in a future context.

The specific research objective is to understand the concept of multi-domain operations and to identify how the combined command and control system operates in the new spectrum of operations. In this sense, the hypothesis underlying the research is that multi-domain operations will create new opportunities to execute command and control actions.

To carry out the research, a qualitative approach was chosen. This approach was considered relevant as it provided an opportunity to deepen certain topics based on the understanding of command-and-control activities in multi-domain operations.

2. Current Approach of Military Operations

Currently, the approach to military operations highlights the use of joint operations, which involve the coordinated use of different categories of forces, with the aim of achieving unity of effort and exploiting the strengths of each category. Advanced technologies such as communication networks, information, surveillance and reconnaissance (ISR) systems, precision guided weapons or unmanned systems are used in the joint operations. These operations involve the integration of non-military actors, such as civilian agencies, non-governmental organizations (NGOs) and international organizations, used in the planning and execution of military actions.

Specific to the met level are campaigns and major military operations. These operations occur as a result of the direct defense of NATO space against any aggressor. This is usually achieved through conventional force-against-force combat of varying scale, frequency and intensity between the armed forces of the structures involved. They act, in principle, as instruments of national or NATO policy, are easily identifiable as combatants, and abide by the laws of armed conflict.

But even major combat operations can be exacerbated, perpetuated or exploited by those who want to benefit from instability through insurgency, terrorism, crime or disorder.

In addition to identifying capabilities, NATO uses the assembled approach to identify potential gaps in the Alliance's collective defense capabilities. This involves analyzing current capabilities and identifying areas where additional resources or training may be needed. By identifying these gaps, NATO can develop a more effective response to potential threats.

NATO also uses the joint approach to develop joint command and control structures. This involves the appointment of a single commander who has the authority to make decisions and issue orders to all categories of forces. This approach aims for all categories of forces to work together for a common objective and their efforts are effectively coordinated.

For its part, Romania has its own doctrine for joint operations, which covers different fundamental aspects specific to this type of operations that take place in certain contexts. Also, the Romanian army regularly conducts joint-type exercises, whether they are planned at the national level or together with NATO or other partner states or structures.

Even though the converging approach has withstood existing challenges for a long time and will likely continue to do so in various forms, certain factors require a change or adaptation in the way military operations are conducted. Innovative weapons and systems underpin the need for commanders to change the way they think about and prepare for war. These technologies include and are not limited to precision strike attack platforms, advanced sensors, intelligent robots, cyber systems, or the use of social media for military purposes. Using them in combination can have two significant effects on the way war is waged: the range of some weapons and

systems will eliminate rigid barriers between domains through their ability to compress the time and space in which military action takes place, and expand the number of domains of war from the traditional three, land, sea and air, to five, with the inclusion of space and the cyber domain, will require greater command integration in what promises to be a more complex environment.

In recent years, technologies have been introduced that have begun to compress domains of warfare and reduce some operational constraints given time and distance. There has always been a degree of overlap between the domains, but over time the areas of overlap between the domains widen to the point where the boundaries between them effectively cease to exist. As the ranges of some systems increase, theater-wide destruction zones will become the norm, not the exception. It is not excluded that these capabilities remain a simple attribute of very powerful states. The more these weapons and systems develop, the more states, even minor ones or some organizations, will acquire a certain ability to project power over long distances.

An example of how the large scale of some systems can redefine the relationships between operating environments is the use of long-range land-launched precision missiles. Although the primary effect may be the danger posed to a fleet, effects of a different order are those that may require changes in the basic principles around which an assembled force is organized. A second-order effect may be that not necessarily the side in a conflict with the strongest fleet will exercise control of the sea, and that this control may be exercised with mobile land-based precision missile platforms.

3. Multi-Domain Military Operations Approach

War evolves, and this is a continuous process over time, military doctrine and strategy also needed to evolve to keep pace

with technological advances, societal changes, and new geopolitical realities. Today, the emergence of new technologies, the changing nature of conflicts and social evolution have led to a new approach to military operations known as multi-domain operations (MDO).

Multi-domain operations represent a new approach to military operations, where the emphasis falls on the integration of all domains of warfare (land, sea, air, cyber and space) to ultimately achieve a common objective. The purpose of these operations is to synchronize and coordinate all operations in all areas, thus creating a well-integrated force that can respond to any emerging threats. Underlying MDO is the premise that no domain can operate in isolation and that success in modern conflicts requires the coordination and integration of all domains.

As can be seen from the above, it was the changing nature of the conflicts that led to the multi-domain approach. Today's conflicts are characterized by complexity, ambiguity and the use of emerging technologies. Military operations are no longer limited to the traditional land, sea and air domains, but are also significantly expanding into the cyber space or even the information domain. Military adversaries use these domains with the aim of disrupting, degrading or denying the capabilities of others, and MDO is a response to all these emerging threats that seeks to leverage the specific capabilities of each domain to create a more comprehensive and effective approach to military operations. State actors are increasingly vulnerable to these threats and must adapt to the changing nature of conflicts.

Emerging technologies such as artificial intelligence, machine learning or autonomous systems offer the possibility of conducting a wider field of military operations. These technologies have the ability to improve situational awareness, to increase the speed of action and agility, but also to reduce the risk to which human

operators are subjected. Even so, they entail new challenges, including the need for new doctrines and forms of training to ensure effective integration.

The current approach to military operations faces challenges from emerging technologies that blur the boundaries between different domains and create new vulnerabilities. For example, the use of cyber-attacks, electronic warfare, and space-based weapons can disrupt communications networks, disable ISR systems, and threaten critical infrastructure. The use of unmanned systems, such as drones and robots, can provide new capabilities for intelligence gathering, surveillance and precision strikes, but can also pose ethical and legal challenges, such as the risk of civilian casualties and accountability for the autonomy of actions. The use of artificial intelligence and machine learning can improve decision-making and speed up operations, but they can also raise concerns about bias, transparency and accountability. The range of cyber and social networking capabilities is even greater than that of missiles. In cyber-attacks, time and distance from an adversary play a lesser role. The ability of such technologies to compress time and space suggests that the existing limiting factor of distance between point of origin and point of effect will soon no longer matter when planning an attack or organizing a defense. So far, no wars have been fought in which the relevance of time and distance is reduced to such an extent (TRADOC, 2018).

A brief review of the newly published American textbook F.M. 3-0 Operations highlights some doctrinal changes and additions, which shows the evolution in updating the doctrine, so that the new multi-domain operations can also be integrated and conducted. The manual provides a solid foundation for the conduct of multi-domain operations by the US military. Some of the newly introduced doctrinal aspects are analyzed below.

The manual introduces an operational environment made up of five physical

domains (land, air, sea, cyber and space) understood through three dimensions (physical, informational and human) (FM3-0, 2022).

Another novelty relates to more principles and imperatives that are applicable to operations. These principles are agility, endurance, depth and convergence.

Agility is defined as *“the ability to move forces and adjust their disposition and activities faster than the adversary”* (FM3-0, 2022). From this principle emerges the importance, for the success of the actions, of the ability to act faster than the opponent.

Endurance is defined as *“the ability to persevere over time and through the depth of an operational environment”* (FM3-0, 2022). This involves using combat power anywhere, for longer periods of time.

Depth is the extension of operations in time space or purpose to achieve definitive results. This focuses on enemy deployment along all domains.

Convergence is *“the denouement created by the concerted use of capabilities from multiple domains and echelons against combinations of decision points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area”* (FM3-0, 2022). The purpose of convergence is to create opportunities that can be exploited.

Imperatives consist of actions that armed forces must perform to defeat enemy forces and accomplish objectives with acceptable losses or costs. These include:

- visualize yourself, visualize the enemy and understand the operational environment. Commanders must possess the ability to view the operational environment in terms of factors relevant to the decision-making process. They must develop a good understanding of their own forces relative to mission requirements, the force's relationship to higher echelons, neighboring forces, and other domains.

Commanders must also try to see themselves from the enemy's perspective, largely by understanding their own critical intelligence elements. The enemy must be viewed in terms of its combat power, advantages and intentions within the operational environment;

- take into account that you are permanently under observation and under the spectrum of all forms of contact; existing air, space and cyber capabilities increase the likelihood that adversary forces will have visual and electromagnetic contact with their own forces. Commanders must operate under the assumption that they are under observation from different domains. Multi-domain operations add a new form of contact, namely influence. It is defined as *“interactions through the information dimension that are intended to shape people's perceptions, behaviors, and decisions about a particular policy or military objective”*;

- create and exploit the physical, informational and human advantage in pursuit of decision-making dominance;

- initiate contact with the smallest possible element; It requires forces to engage with sensors or unmanned systems to minimize risk to key personnel and capabilities;

- impose multiple dilemmas on the enemy. This imperative assumes that by applying the capabilities in a complementary way to create more problems for the adversary than it is capable of solving;

- anticipate, plan and execute transitions. Commanders must identify potential transitions early in the planning process and take them into account. It creates stable changes, especially in the human and informational dimension.

- designate, weigh and sustain the main effort.

- permanently consolidate gains. The multi-domain side of the operational environment puts high pressure on the

ability of military forces to create lasting change especially in the human and informational dimensions. Commanders must always judge when and how to consolidate their gains as the situation develops;

- understand and manage the effects of operations on the military (FM3-0, 2022).

Viewed from the perspective of the United States, the MDO is a key factor in both the national interest and NATO's mission to deter and defend against any threat that may come from state or non-state actors. The US is the first military power to understand and recognize the need to adapt to the current security environment and develop new concepts and capabilities to maintain its edge in the face of emerging threats. The US approach to the MDO is based on the principle of "*superiority in all domains*", which implies that NATO most likely also aims to achieve superiority in all domains, including land, sea, air, space and cyberspace. Superiority in all areas requires the integration of different categories of forces, the use of advanced technologies and cooperation with allies and partners.

To achieve superiority in all fields, the US is pursuing several initiatives. One of these is Joint All-Domain Command and Control (JADC2). It represents a modern military concept, which allows the integration of all domains in the current battlefield. It brings together all operational domains, even space and cyber, and ensures seamless cooperation not only at the national level, but also between NATO member countries. JADC2 is designed to provide the joint force commander with the tools necessary to effectively control and manage operations in a multi-domain environment (Hoehn, 2022).

One of the key aspects of JADC2 is misrepresentation. In the context of multi-domain operations, deception is very important to confuse the enemy and prevent him from understanding the real intentions

of the military, in this case the US, in the event of potential military actions.

JADC2 is designed to enable the effective use of deception by integrating information from multiple sources and domains, enabling the joint force commander to make informed decisions quickly. By using advanced technologies such as artificial intelligence, machine learning and big data analysis, JADC2 provides a more comprehensive picture of the battlefield, allowing the US to mislead the enemy in an effective manner.

JADC2 also allows for the coordinated use of deception in multiple domains. This implies that deception operations can be conducted simultaneously on land, sea, air, space and cyberspace. By creating a consistent narrative of misrepresentation with elements from all areas, the likelihood of success using this process increases.

Another aspect of JADC2 that is related to deception is the ability to quickly change techniques and tactics as needed. In a multi-domain environment, the situation can change quickly and the ability to adapt quickly is essential. JADC2 provides the joint force commander with real-time data and analysis, allowing him to rapidly adjust his deception tactics and techniques to meet changing circumstances. This allows the US to keep the enemy off balance, making it difficult for him to discern the intentions of US forces. Furthermore, JADC2 enables the joint force commander to effectively communicate with forces in all domains. This is essential in the coordination of deception operations, as it allows the dissemination of false information in a coordinated and timely manner. With JADC2, the joint force commander can ensure that all troops are aware of the deception scenario and narrative and understand their role in accomplishing it.

Joint All-Domain Command and Control (JADC2) is an essential military concept for the evolution of multi-domain

operations, enabling the integration of all operational domains on the modern battlefield. It is the key enabler of deception in multi-domain operations, as it provides the joint force commander with the necessary tools to effectively control and manage operations in all environments. Based on the use of advanced technologies such as artificial intelligence, machine learning and big data analysis, JADC2 provides a more comprehensive view of the battlefield, enabling more effective deception operations. In addition, JADC2 enables the use of deception in multiple domains, the ability to rapidly change tactics and techniques, and effective communication with troops in all domains, all of which are critical to the successful conduct of deception operations.

Multi-domain operations have been identified as a key component in the US military's development strategy, as well as in NATO's new regional defense plans, the purpose of which is to create the conditions to better respond to current threats.

NATO would intend to use the MDO concept for regional defense plans in several specific ways, such as:

- Identifying and exploiting the unique capabilities of each field; one of the key aspects of the MDO concept is the recognition that each domain has unique capabilities that can be leveraged to achieve a common goal. NATO intends to use this approach to identify and exploit the unique capabilities of each domain to achieve the strategic objectives of its Regional Defense Plans;

- Coordination of actions between fields; another important aspect of the MDO concept is the need for coordination between domains. NATO intends to use this approach to ensure that actions taken in one area are coordinated with actions taken in other areas to achieve a coordinated and synchronized response to potential threats;

- Integration of information between domains; the MDO concept also recognizes

the importance of integrating information across domains. NATO intends to use this approach to ensure that information gathered in one domain is disseminated to other domains in a timely and effective manner to gain a more comprehensive and accurate understanding of potential threats.

- Development of joint command and control structures; NATO intends to use the MDO concept to develop common command and control structures that enable more efficient and effective domain decision-making. This will help ensure that all areas focus their efforts towards a common goal and that these efforts are coordinated and synchronized.

- Conducting joint exercises; the MDO concept emphasizes the importance of training and joint exercises to ensure that all domains are familiar with the capabilities and limitations of the other domains. NATO plans to use this approach to develop forms of training and exercises that will improve coordination and synchronization across domain.

- Adaptation to emerging threats; the MDO concept recognizes that potential threats can arise from any domain and that the nature of these threats is constantly evolving. NATO intends to use this approach to remain agile and adaptable in the face of emerging threats by leveraging the unique capabilities of each domain to respond to potential threats in a coordinated and synchronized manner.

- Improving NATO's defense posture; by leveraging the MDO concept, NATO intends to enhance the overall posture of its defense posture, ensuring that all domains are used for a common objective and that efforts are coordinated and synchronized.

4. Conclusions

At the present time, the mental challenge facing military organizations to adopt a multi-domain mindset is very high, as it involves a significant adjustment of force structure and organizational requirements.

The transition from the collective to the multi-domain way of thinking involves, among other things, some difficulties. Commanders of the future will need different skills than those needed today. They must lead the structure they lead to victory in the chaos of the multiplicity of domains where some of the traditional boundaries no longer exist, look at war through the lens of integrated domains, and understand how they can wreak havoc on an enemy by putting him in the face of complicated situations from several

domains, thus overwhelming his ability to understand, react and survive.

Multi-domain operations present both challenges and opportunities in various areas, such as military education, wargaming, organizational culture. How NATO member countries adapt their national approach to the multi-domain approach will have an impact on operational success. As part of military actions, deception will be affected to some extent by the new changes.

REFERENCES

AJP-3. (2019). *Allied Joint Doctrine for the Conduct of Operations*. Bruxelles: NATO Standardization Office.

F.M. 3-0. (2022). *Operations*. Washington DC: Headquarters Department of the Army.

Hoehn, J.R. (2022). *Joint All-Domani Command and Control (JADC2)*. Available at: <https://sgp.fas.org/crs/natsec/IF11493.pdf>

NATO. (2023). *Operations and missions: past and present*. Available at: https://www.nato.int/cps/en/natohq/topics_52060.htm

TRADOC. (2018). *The U.S. Army in Multi-Domain Operations 2028*. Available at: <https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf>