DOI: 10.53477/1842-9904-22-14

ACHIEVING INTER-DOMAINS EFFECTS – CHALLENGE IMPOSED BY THE MULTI-DOMAIN OPERATION

*Alexandru-Lucian CUCINSCHI**
*Ion CHIORCEA, PhD***

The multi-domain operation, although still insufficiently developed from a theoretical and, above all, practical point of view, can summarize the paradigm shift produced at the strategic level, a change caused by the developments in the current security environment. However, although this type of operation includes new types of technologies developed mainly as a pragmatic need by the tactical level and aims to achieve coherent solutions to counter the A2AD (anti-access and interdiction) threat at the strategic level, the coordination of the aspects necessary to carry out such operations currently seem rather difficult to achieve by the operational level, which aims at innovatively combining the specific tactics of the services to achieve operational and strategic level objectives. We consider that what is currently lacking as a tool for planning and conducting military actions is how to achieve inter-domains effects. Thus, in this article we will analyze the extent to which obtaining inter-domains effects in multi-domain operations can represent the necessary binder to implement such an operation.

Keywords: *military art; multi-domain operation; inter-domain effects; military action.*

**** Commander (N) Instructor Alexandru-Lucian CUCINSCHI is a PhD Student at the "Carol I" National Defence University, Bucharest, Romania. E-mail: cucinschi.alexandru@gmail.com***

***** Captain (N)(Ret.) Ion CHIORCEA, PhD, is a Professor at the "Mircea cel Bătrân" Naval Academy, Constanța, Romania. E-mail: chiorcea44@yahoo.com***

Introduction

The implementation of the multi-domain operation entails many challenges, as they are not limited to the integration of two new domains (cyber and space) within a conventional joint operation, and are of a complexity that in many cases exceeds the synthesis capacity of the current tools used by the military for planning and conducting military actions.

Thus, although initially the idea of integrating the two domains by the services was envisaged, at the tactical level, as the examples show: US Land Forces - US Land Forces in multi-domain operations 2028 (TRADOC, 2018); UK Air Force, by reforming the air groups so that they are able to respond to multi-domain threats (RAF, 2018) – one senses even from the ad hoc approach, at the level of the force categories, the necessary breadth to carry out such operations.

In this respect, the multi-domain operation has subsequently been approached mainly at the strategic level and less at the operational level, considering, first of all, its scope (it must be able to encompass the space and cyber domains, which are not entirely under military control). In addition, if at the tactical level some tools can be intuited by which new tactics can be deduced through exercises and experimentation and at the strategic level the goal, means and ways of achieving the goal are mostly known, at the operational level it is still quite difficult to determine how the actions of the services can work together to achieve strategic level objectives within the multi-domain operation.

However, the ways of implementing the multi-domain operation at the strategic level – NATO Warfighting Capstone Concept (Tammen, 2021); Integrated Operating Concept (UKMOD, Integrated Operating Concept, 2021) – shed light on expectations at the operational level. These, combined with the elements developed by the services in terms of multi-domain operation, can help identify the implications for the operational level.

Thus, operational-level concepts, such as Joint All Domain Command and Control (JADC2), which involves connecting sensors from all services into a single network with the aim of shortening decision-making time (CRS, 2022), aim to solve an operational-level problem: joint force command and control.

Similarly, the NATO Warfighting Capstone Concept, previously mentioned as a reference document for the strategic level, outlines five imperative directions for the development of combat (Tammen, 2021) including inter-domain command, leading to a dilemma as to the level at which the multi-domain operation can be managed from a command and control (strategic or operational) point of view.

The question is whether JADC2 (which we consider an operational level concept), which actually details the inter-domain command stipulated in the NATO Warfighting Capstone Concept (strategic level), is sufficient to bring the necessary functionality to the operational level in the current security environment. In other words, is streamlining force command and control enough to gain an operational advantage over the adversary?

Based on the study, from the historical perspective of both the joint operation and the elements known to date about the multi-domain operation, we appreciate that the streamlining of command and control, although necessary, is not sufficient to provide the necessary coherence for the operational level so that it can be able to manage complex situations in a dynamic difficult to anticipate.

Thus, the hypothesis that we propose to test in this paper is as follows: If tools can be identified to achieve inter-domain effects, can the multi-domain operation contribute to the fulfillment of strategic objectives under the conditions imposed by the current security environment?

In order to so, we will analyze the known elements about the multi-domain operation at the tactical and strategic-military levels, then we will identify the challenges that the current security environment imposes on the operative level, and attempt to identify whether in the current security context the achievement of inter-domains can represent a viable tool for planning and conducting military actions at the operational level.

1. The Peculiarities of the Multi-Domain Operation at Tactical Level

Although in many cases the tactical level has overtaken the higher levels of military art in the sense of pushing the limits of the forces available through the initiatives of commanders, greatly influencing the fate of a conflict, nevertheless, as the current conflict in Ukraine has demonstrated, war won by a decisive battle is no longer possible in the vast majority of cases (Freedman, 2019).

An example of this is the Blitzkrieg, which, in the first part of the Second World War, contributed greatly to the successes of the German Army (the invasion of Poland, Denmark, Norway, Holland (the Netherlands), Belgium and France). Thus, the German Army, benefiting from the lessons identified in the past (von Moltke was a proponent of delegating authority to commanders at different levels), successfully applied this type of concept, a relevant example being the actions undertaken by General Heinz Guderian during the invasion of France. The latter, although he had been warned not to advance before sufficient infantry divisions had been brought into the battlespace in support of the armoured ones, after heated discussions with his superiors, sensing that the French were in disarray, advanced, paralyzing the French defence (Beevor, 2015). “So what would be erroneously described as a blitzkrieg strategy was largely an on-the-spot improvisation” (Beevor, 2015).

Currently, this type of tactical actions can only be carried out in the face of a clearly inferior adversary, in terms of combat power, considering the fact that with the end of the Cold War, the Armed Forces ceased to represent a factor of progress in the technological field and the civilian/private sector took over this position. Thus, not having the most advanced technologies at their disposal, the military instrument of power began to depend to a large extent both on the state's other instruments of power of and on the large companies that develop new technologies for commercial purposes, but whose military applicability cannot be ignored.

As a result, at the tactical level, we consider that by promoting the multi-domain operation, there is an incorporation of new technologies into the tactical framework specific to each service, with the aim of identifying new ways of action.

Thus, the fact that the **Naval Forces** have come to the conclusion that, for practical reasons (involving risks) some of their actions can be executed by unmanned platforms, which can operate in all three specific environments (surface, submarine and air), is an aspect from which multi-domain operation can benefit in countering A2AD.

Also, artificial intelligence, by processing data from different sources (large databases), has led to improved maritime situational awareness, a fact that can indicate practical solutions, at a tactical level, for addressing concrete situations in the maritime domain that higher hierarchical levels (operational and strategic) need to consider.

However, if the incorporation of new methods of conducting military actions at the tactical level can bring the actions of the Naval Forces up to date with the specific reality of the maritime domain, in order to fulfil operational and strategic objectives, we consider that this must be accompanied by the development of new capabilities which will contribute to the implementation of the multi-domain operation in its ensemble.

The US **Army**, by publishing TRADOC Pamphlet 525-3-1−The US Army in multi-domain operations 2028, deals with the issue of the multi-domain operation more from a strategic and operational perspective and less at the tactical level, with the threat (A2/AD implemented by Russia and China) as the basis for the development of this operation.

However, the role of technology, although presented in terms of the possibilities available to potential adversaries, is considered as an essential premise in the development of the multi-domain operation: the proliferation of precision-guided weaponry, integrated air defence systems, cyberspace-specific weaponry, and other technologies enable a large number of potential adversaries to challenge and pose a risk to US Armed Forces in all domains, including the electromagnetic spectrum and the information environment at the tactical, operational, and strategic levels (TRADOC, 2018).

For the **Air Force**, a number of weapons companies have moved to develop solutions for implementing new technologies, both within existing military equipment and as new weapon systems that can operate in the battlespace. It is worth noting that this equipment is being developed in the sense dictated by the multi-domain operation, to operate in several domains and inter-domains.

Thus, the Leonardo company offers specific weapon systems for multi-domain operations in addition to combat aircraft and helicopters equipped with state-of-the-art equipment and sensors, unmanned aerial vehicles (Falco EVO UAV) that can carry out a wide range of missions on land as and at sea thanks to innovative sensors, complete information integration solutions with surveillance data and modular avionics capable of managing a wide range of sensors, with the aim of accelerating and optimizing the decision-making process. The same company also offers solutions in the field of electronic warfare, such as the SAGE system (can be installed on a wide range of airborne platforms), which analyzes the electromagnetic spectrum in the air, land and sea environments to identify emissions sources and implicitly targets (Leonardo, 2022).

Airbus provides the military with systems that can counter cyber-attacks (MTLID) for the protection of military networks and data; unmanned aerial platforms (Aliaca UAS); IT solutions such as the multi-domain combat cloud, a tool that facilitates, by achieving information superiority, the collaboration of manned and unmanned vehicles during combat, in all environments (Airbus, 2022).

From the mentioned, we believe it can be stated that the tactical level has begun to incorporate new technologies into the specific capabilities of each service, with the observation that this process has been accelerated precisely by the affirmation of the intention to develop a new type of operations by the Armed Forces and the broad outline of its defining elements through the publication of studies and doctrines in this regard.

We thus observe that the development of this new concept, although based on new technologies that can be implemented by the tactical level, is not limited to them and also implies a statement of intent that, as is only natural, comes from the strategic level.

2. Contribution of the Strategy to the Development of Multi-Domain Operation

The strategic level, defined by different approaches, is best represented by two components that must be separated, given the specificity of each: strategic-political and strategic-military.

The strategic-political level is the one that launches the declaration of intent, as is the case of the multi-domain operation today, and it is responsible for the highest spheres of addressing relations between the actors (state and non-state) that dispute their primacy in different fields, including the military (where the issue of conflicts is also addressed).

Although most geopolitical and geostrategic specialists believe that „geopolitical disputes and rivalries start from the idea that in the globalizing international environment, economic means, and not necessarily military ones, are those that guarantee control, such as: access to stock market values from abroad; private direct investments; control of local currency reserves (either through the IMF and World Bank, or through multinational corporations in less developed countries); control of mineral resources, agriculture, manufacturing and other goods; and, last but not least, the organization and management of trade through foreign corporations" (Hlihor, 2005), we consider it our duty, as military personnel, to manage the ways in which the military tool can be used in support of economic means, but also as the main tool in case the economic means do not achieve the expected effect.

This declaration of intent is usually promoted through military strategy, although, as mentioned, the military instrument does not always play a central role, because it is the military that will ultimately guarantee the implementation of this strategy or, if this guarantee will not be considered effective, will move to forcing things in the direction established by the decision-makers at the strategic-political level.

Thus, we believe that a certain definition is relevant, from the perspective of identifying the defining element specific to military strategy: „military strategy consists of establishing military objectives and formulating strategic concepts for their fulfilment by using military resources to implement the concepts." (Potîrniche, 2020).

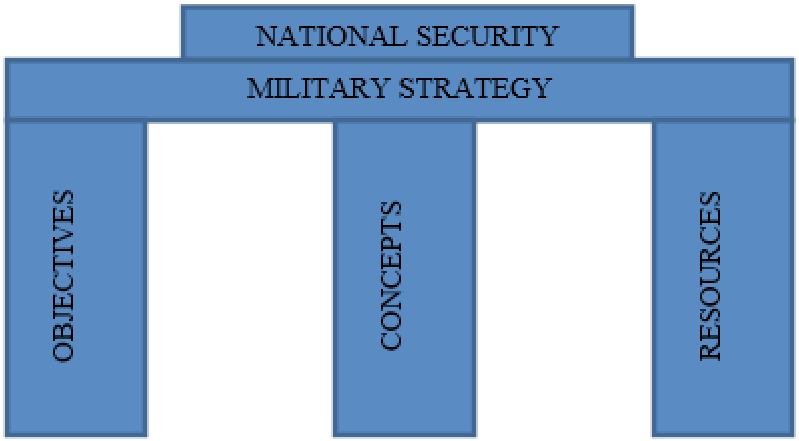


Figure no. 1: Military strategy components (Potîrniche, 2020)

Having presented, in Figure no. 1.1, the pillars on which the military strategy rests, we believe that it can be understood that setting the objectives does not require a special intellectual effort because, in most cases, it is quite easy to intuit what should be perform to reach a desired end state. Also, the issue of resources, although complex and may involve considerable administrative efforts, depends more on organizational capacity and does not require a special intellectual effort.

On the other hand, the development of concepts, which in our opinion represent the essence of strategy, requires intense intellectual effort, and although it is difficult to quantify the outcome of this effort, we believe that the military's main responsibility is to understand how these concepts give a meaning to strategy and contribute to their continued development or improvement.

Currently the military strategy of NATO and most NATO member states and partners focuses on the design, development and application of the multi-domain operation concept. We are thus witnessing what is considered to be a process of military modernization based on this concept. This entails, firstly, an analysis of the future operating environment (where the threat is, in fact, the main element that is taken into account), then the identification of a concept (an idea that summarizes reality) and, finally, the development of new capabilities to be able to support the implementation of the concept, thus leading to countering the threat.

In the case of the multi-domain operation, A2AD represents, as with previous concepts (starting with the air-sea battle – 2009) the military problem that the US military must solve. A2AD capabilities have been considered those that threaten the ability of US and allied forces to get into a position to fight (access denial) as well as to fight effectively once in that position (maneuver denial) (ASBO, 2013).

Regarding the clarity of explanation of the A2AD concept, we find the following definitions of A2AD to be illuminating:

– A2 - action aimed at slowing down the deployment of own forces in a theatre of operations or forcing them to operate at a distance from the area where they would have been indicated to position themselves (affects movement);

– AD - action aimed at preventing own forces from operating in an area of operations where an adversary is unable or unwilling to deny access (affects the maneuver) (ASBO, 2013).

We notice that A2 hinders advantageous positioning, which is one of the components of operational planning, along with tactics and logistics, while AD prevents effective tactics, which indicates that *there will be great difficulties in operational planning*, logistics being also in a position to encounter difficulties if not addressed in time.

In response to this threat, the US, which has currently presented the most programmatic documents regarding the multi-domain operation, proposes a comprehensive approach of this type of concept, placing it at the strategic level, with implications for the operational level, while at the tactical level there is only the issue of multi-domain formations.

This is indicated by the division of the operation into phases: Competition, Penetration, Disintegration, Exploitation and Competition on favourable terms

(TRADOC, 2018). Analyzing, in the reference document mentioned, the aspects that make up these phases, we observe the extent necessary to command and control such an operation, an aspect that, in our opinion, cannot be managed by a level lower than the military-strategic level.

However, the military-strategic level cannot manage the correlation of tactics specific to each service, to which the cyber and space domains are currently added. This is the prerogative of the operational level, which, as von Moltke described it, as the level at which the military must not expect any political interference, must be able to achieve synergy (in the case of joint operation) and, more recently, convergence (in the case of multi-domain operation).

3. Multi-Domain Operation at Operative Level – Inter-Domain Effects

It is the operational level that must ultimately integrate, in a coherent way and adapted to the current threat, the tactics specific to the categories of forces, to which positioning and logistics are added. Operational planning is primarily the achievement of strategic goals by large combat units through a combination of positioning, tactics, and logistics (Skinner, 1988).

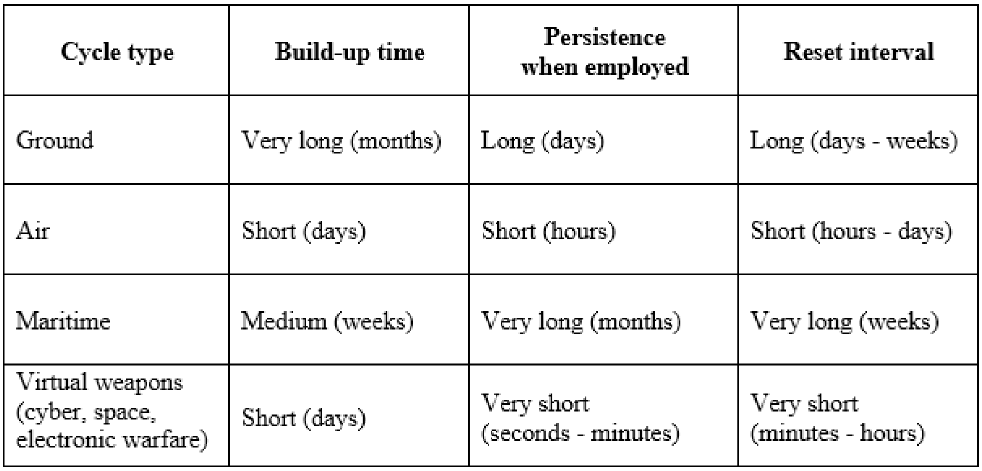
However, in addition to the military-strategic level threat, there is a threat specifically created for the operational level. Thus, the A2AD component, which aims at separating the joint force in time, space and combat functions, made the classic joint operations no longer possible to conduct except in an uncontested environment. Thus, high-precision, long-range weapon systems protected by anti-aircraft systems (both in multiple layers) create great problems for the joint force, both on the offensive and the defensive, with support between the services difficult to achieve. This is also the reason why, in order to compensate for these vulnerabilities, the cyber environment (2016) and later the space environment (2019) were first recognized as operational domains from which an advantage can be ensured for forces fighting in conventional environments. Moreover, these two environments can generate capabilities that can fight in place of some of the capabilities specific to conventional environments. This is what we consider of inter-domain effects.

As a result, we believe that following the model of the two new domains, this process should also be implemented within the classical environments, in order to successfully counter the A2AD threat at the operational level.

In this regard, in a previous personal paper, I suggested the following definition for the multi-domain operation at the operational level: “The ability of a service to temporarily fight in the specific domain (environment) of another service in order to provide an operational advantage with the aim of regaining/winning the initiative in that environment/domain” (Cucinschi, 2021).

We believe that by applying these inter-domain effects, it is possible to counteract, in the first phase, the separation of forces in time, a separation which, due to the specific nature of each category of forces, is easily exploited by the adversary (Table no. 1).

Table no. 1. Characteristics of the ground, air, maritime, and enduring virtual weapons cycles (TRADOC, 2018)



Cycle type	Build-up time	Persistence when employed	Reset interval
Ground	Very long (months)	Long (days)	Long (days - weeks)
Air	Short (days)	Short (hours)	Short (hours - days)
Maritime	Medium (weeks)	Very long (months)	Very long (weeks)
Virtual weapons (cyber, space, electronic warfare)	Short (days)	Very short (seconds - minutes)	Very short (minutes - hours)

After this separation in time (if successful) one can move to full control of an environment, which can allow exploitation of success in that environment, thus reaching the separation of combat and space functions.

This is the main reason why we believe that obtaining inter-domain effects is vital for multi-domain operation. If the separation in time succeeds for the adversary, the main advantage of the multi-domain approach to the operation, represented by the multiple options of own forces that turn into multiple dilemmas for the adversary, is nullified, the multi-domain operation thus tending towards a classical joint operation without much chance of success.

In the same vein, the UK Ministry of Defence has attempted, by publishing Joint Concept Note 1/17 – Future Force Concept, to explore the new relationships that can be established between or along the domains (UKMOD, Joint Concept Note 1/17 - Future Force Concept, 2017).

Conclusions

We consider that, unlike JCN 1/17, where inter-domain integration is considered sufficient to combat multiple threats in a single environment, to impose coherence on the actions of own forces as a whole, as a joint force and, and to build the capabilities appropriate to a certain type of threat, the issue to explore and develop the best practices in terms of controlling spaces that until recently were inaccessible to them.

Because only by producing a pre-planned, intentional effect (as a result of an action) in the domain/environment specific to another service or in one of the two new domains (cyber and space) it is possible to determine the proportion of capabilities required for each domain as well as to identify asymmetric employment possibilities (the multitude of possible combinations), we appreciate that the inter-domain effects should be exploited in the sense of identifying them in time as well as the possibilities for their innovative combination.

By exploring these inter-domain effects, it is possible to build capabilities appropriate to concrete situations in a given geographic space, thus leading to what we have highlighted in Figure no. 2, within the tactical level – multi-domain formations, units that are area-specific, taking into account both the physical environment and the opponent.

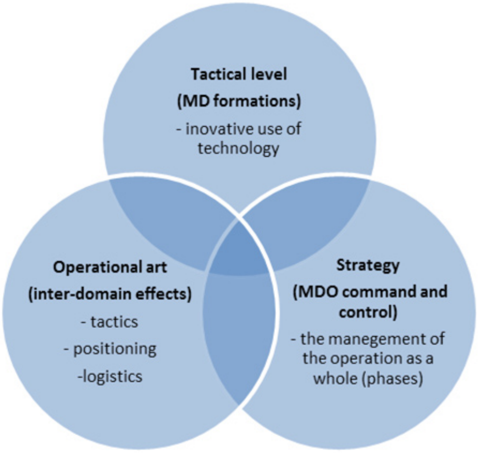

Tactical level
(MD formations)
- inovative use of technology
Operational art
(inter-domain effects)
- tactics
- positioning
-logistics
Strategy
(MDO command and control)
- the manegement of the operation as a whole (phases)

Figure no. 2: The implications of multi-domain operations to the military art components

In addition to the possible implications mentioned, we believe that it should also be highlighted that the current operations planning process (effects-based planning through the use of operational design) will have to undergo some changes, not only in the sense of integrating effects produced by the actions of one service in the specific domain of another service into the operational level design, but also in the sense of making the design elements more flexible, as they are currently increasingly rigid due to the computerization of decision-making, with computing machines leaving few aspects to the discretion of commanders.

BIBLIOGRAPHY:

Airbus. (2022). *Airbus Company*. Retrieved Octomber 7, 2022, https://www.airbus.com/en/newsroom/stories/2022-06-airbus-brings-leading-edge-digital-capabilities-to-multi-domain-military.

ASBO. (2013). *Air-Sea Battle Office. Air-Sea Battle, Service Collaboration to Adrdress Anti-Access&Area Denial Challenges.*

Beevor, A. (2015). *Al Doilea Război Mondial.* București: Editura RAO.

CRS. (2022). *Congressional research Service.* Retrieved July 19, 2022, athttps://sgp.fas.org/crs/natsec/IF11493.pdf.

Cucinschi, A. (2021). *Operația întrunită și operația multi-domeniu – Delimitări conceptuale.* București: Biblioteca Universității Naționale de Apărare "Carol I".

Freedman, L. (2019). *Viitorul războiului, o istorie.* București: Editura Litera.

Hlihor, C. (2005). *Geopolitica și geostrategia în analiza relațiilor internaționale contemporane.* București: Editura Universității Naționale de Apărare "Carol I".

Leonardo. (2022). *FIDAE 2022: Leonardo's multi-domain technologies to meet every operational need.* Retrieved Octomber 7, 2022, https://www.leonardo.com/en/news-and-stories-detail/-/detail/fidae-2022-leonardo.

Potîrniche, M. T. (2020). *Teorii și concepte strategice – Evaluarea prospectivă a stretegiei militare. Viitorul strategiei militare.* București: Editura Universității Naționale de Apărare "Carol I".

RAF. (2018). *Historic 11 Group reforms for multi-domain challenges.* Retrieved july 18, 2022, de pe https://www.raf.mod.uk/news/articles/historic-11-group-reforms-for-multi-domain-challenges/

Skinner, D. (1988). *Airland Battle Doctrine, Center for Naval Analysis.*

Tammen, J. W. (2021). *NATO's Warfighting Capstone Concept: anticipating the changing character of war.* Retrieved July 19, 2022, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

TRADOC. (2018). *TRADOC Pamphlet 525-3-1 – The US Army in multi-domain operations 2028.* Retrieved july 18, 2022, https://adminpubs.tradoc.army.mil/pamphlets/TP523-3-1.pdf.

UKMOD. (2017). *Joint Concept Note 1/17 – Future Force Concept.*

UKMOD. (2021). *Integrated Operating Concept.* Retrieved July 19, 2022, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1014659/Integrated_Operating_Concept_2025.pdf.