Conceptual Approach to Multi-Domain Operations

Koncepční přístup k multidoménovým operacím

Zdeněk Petráš

Abstract: This article delves into multi-domain operations in the context of future warfighting. A multi-domain approach to operations is being progressively implemented in allied nations and within NATO, as well. It should also become a core interest for the Czech Republic, even if the sea and space domains do not represent the crucial area of potential operational engagement of the Army of the Czech Republic. The complexity of operations in a complex operating environment requires mutual interaction across all operational domains. The integration of the physical and virtual spheres of operations suggests that operations planning cannot be strictly oriented to individual operational domains. The interaction between operational domains must be perceived as a sine qua non for effective planning and conducting military operations. This is also a fundamental prerequisite for the successful activity of forces in a complex operating environment.

Abstrakt: Cílem článku je představit koncepci vícedoménových operací v kontextu moderního strategického myšlení a moderního válečnictví. Multidoménový přístup k vedení operací je předmětem implementace v aliančních zemích i v rámci NATO. Měl by se tedy stát i předmětem výrazného zájmu v České republice, a to i za situace, kdy především námořní a vesmírná doména nepředstavují hlavní sféru operační činnosti AČR. Složitost soudobých operací vyžaduje zajištění vzájemné interakce napříč všemi operačními doménami. Integrace fyzické a virtuální sféry operací naznačuje, že pohled na plánování operací již nelze striktně omezovat na jednotlivé operační oblasti. Interakce mezi operačními oblastmi musí být vnímána jako stěžejní podmínka pro efektivní obranné plánování, rozvoj schopností, a nakonec i pro plánování a vedení vojenských operací. I to je základním předpokladem pro úspěšnou činnost ozbrojených sil ve složitém operačním prostředí.

Key Words: Strategy; Multi-Domain; Operating Environment; Multi-Dimensional.

Klíčová slova: Strategie; multidoménové operace; operační prostředí; multidimenzionální,

INTRODUCTION

This article is conceived as a compilation of key findings stemming from conceptual documents of those countries that are systematically involved in this issue. Besides the United States, which has already fully implemented the concept in the US Army, the main focus is concentrated on the conceptual approach of the UK, France and Italy. In addition to these countries, the detailed approach of NATO and the EU was scrutinised as well because both Alliance collective defence and the EU Common Security and Defence Policy are facing a need for internal adaptation to operations potentially taking place in a multi-domain environment.

Multi-domain is the term which has been largely used in recent years, especially to integrate the new domain - cyberspace[1] - within the traditional operation domains, i.e. land, sea, air and space. However, this fact even more accentuates the complexity of the multidomain. In past conflicts, retrospectively, everything used to be so simple. There was only the Navy and the Army fighting enemies on land or sea, and then the new flying machines now zooming higher into space. In the past conflicts, it used to be all so simple. There was just the navy and army fighting enemies on land or sea, and then new flying machines, now zooming higher into space. However, these traditional armed services and their traditional fighting domains reflect only a mono-dimensional view of influence projection in a physical dimension. Today's information-age cyber and social operations take place in the information dimension and these are specifically designed to deliver expected achievements in the cognitive dimension. The expired mono-dimensional approach and strategic thinking are constraining and limit modern manoeuvring capabilities to fight the forthcoming multi-domain conflict. This conflict will also require multi-dimensional, not just multi-domain strategic thinking.

Defining multi-domain operations and understanding their scope in terms of transformational needs primarily requires an understanding of the paradigmatic shift that differentiates them from traditional joint operations. These are based on the need to achieve superiority in the area of competence through the ability of individual components to function in a coordinated manner. Therefore, while aiming for some degree of interoperability, it mandates individual components to perform activities in their reference environment, while ensuring a clear demarcation between domains that are generally considered to be adjacent to each other.

On the other hand, multi-domain operations base their essence on the knowledge that it is not possible to maintain superiority in all domains against an equal competitor. Therefore, they aim to maintain freedom of action in all domains to seize any opportunity through the convergence of effects to be achieved by synchronizing actions across domains. In particular, if necessary, the development of autonomous actions by a single component, limited in time and space, can be assumed to create a window of

---

[1] Cyberspace was identified by NATO as a domain at the NATO Warsaw Summit in 2016. The Alliance recognized that a cyber-attack can cause damage comparable to an armed attack and therefore can become a case of collective defence within the meaning of Article 5 of the Washington Treaty.

opportunity for the benefit of other components. The multi-domain approach therefore innovatively redesigns multi-domain operations to produce effects through the simultaneous combination of different capabilities, assuming that the context of the reference is to be understood as unique. This is because each domain has unique characteristics that affect the forces, abilities, personnel, and weapon systems that operate within it.

In particular, the three classic domains (land, sea, and air) are widely interconnected, which might not facilitate the conduct of a multi-domain operation.

1 METHODOLOGY

A comprehensive analysis of the operational domains and multi-domain operations in the context of modern strategic thinking and modern warfare is part of broader research conducted by the Centre for Security and Military-Strategic Studies. It is of note that a detailed description of the scientific methodology used for mapping, summarizing and assessing national and multinational approaches is the subject of this article. However, the summary of complex outcomes cannot be incorporated into this article due to their extent and complexity. All outcomes of the analytical research are available at the Centre for Security and Military-Strategic Studies if need be.

To extract substantial findings, the databases managed by respective national, NATO and EU institutions were used for identifying relevant documents (see Table 1 - the survey of databases exploited for literature research). Based on the identified subject matter publications (see Table 2), the literature review and content analysis were conducted with a view to identifying those findings which closely deal with the operating environment, operational domains and approaches to multi-domain operations. Appropriate findings, basically in the form of integral text in sentences or paragraphs, were then gathered in clusters reflecting affiliation to one or more operational domains. The next step lay in applying the qualitative content analysis, aimed at identifying military capabilities being prospectively required in individual operational domains

Once the phase of findings identification from relevant publications is complete, respective data and information were aggregated in accordance with patterns characterising position in the operational domain framework.

As a final stage, the resulting synthesis of individual findings from national analyses and from the analysis of development trends in NATO and the EU was confronted with the conclusions that emerged from the analysis of the Defence Strategy of the Czech Republic. This phase of the study, in the end, should furthermore enable to identification of crucial implications for the Armed Forces of the Czech Republic in terms of upcoming military capabilities required for successful engagement in joint operations in respective operational domains.

Table 1: Databases exploited for literature research

|	
US Defense Technical Information Center	https://discover.dtic.mil/
UK Defence and Armed Forces	https://www.gov.uk/defence-and-armed-forces
Institut de Recherche Stratégique de l'Ecole Militaire – IRSEM	https://www.irsem.fr/
Istituto di Ricerca e Analisi della Difesa -IRAD	https://www.difesa.it/SMD_/CASD/IM/CeMiSS/Pagine/default.aspx
Joint Air Power Competence Centre – JAPCC	https://www.japcc.org/
NATO Science and Technology Organization - NATO STO	https://www.sto.nato.int/Pages/default.aspx
European Union Institute for Security Studies – EU ISS	https://www.iss.europa.eu/
European Commission JRC Publications Repository	https://publications.jrc.ec.europa.eu/repository/

Table 2: Outcomes of Literature Research

NATO	JAPCC (ed.). *Shaping NATO for Multi-Domain Operations of the Future*. Conference Proceedings. Kalkar: Germany. 2019.
NATO	HEREN, Henry. *Multi-Domain Operations: Inconceivable!* The Journal of the JAPCC, Edition 29, Winter 2019 /2020. Kalkar: Germany.
NATO	JAPCC (ed.). *All-Domain Operations in a Combined Environment*. Multi-Domain Operations. The Journal of the JAPCC. 2021. Kalkar: Germany.
NATO	JAPCC (ed.). *Multi-Domain Operations: Inconceivable!* Multi-Domain Operations. The Journal of the JAPCC. 2020. Kalkar: Germany.
NATO	NATO STO (ed.). *Capability Planning.* Paris, France: NATO Science and Technology Organization, 2018, 58 p. ISBN 978-92-837-2153-6.
NATO	GLARUM, Sigurd, Alf-Christian HENNUM. *RTO-MP-SAS-081 - Analytical Support to Defence Transformation: J-DARTS - An End-to-End Defence Planning Tool Set*. Paris, France: NATO Science and Technology Organization, 2010, 404 s. ISBN 978-92-837-0116-3.
NATO	NATO STO (ed.). *Joint operations 2030*. Neuilly-sur-Seine Cedex: NATO, Research and Technology Organization, 2011. ISBN 9789283701286.
EU	COUNCIL OF THE EU (ed.). *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*. General Secretariat of the Council, 7371/22. Belgium, Brussels, 2022
EU	MEYER Christoph, Ton VAN OSCH, Yf REYKERS. T*he EU Rapid Deployment Capacity: This time, it's for real?* Policy Department for External Relations Directorate, General for External Policies of the Union. PE 702.568 - October 2022. Belgium: Brussels
EU	CULLEN, P., Juola, C., KARAGIANNIS, G., KIVISOO, K., NORMARK, M., RÁCZ, A., SCHMID, J., SCHROEFL, J. *The Landscape of Hybrid Threats: A Conceptual Model*. UE Hybrid Centre of Excellence (CoE). EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-56943-5, doi:10.2760/419776, JRC123305.
EU	COUNCIL OF THE EU (ed.). *EU Guidance on countering Hybrid threats during the planning phase of EU-led CSDP military operations and missions*. EEAS. 8448/21. Brussels: Belgium. 2021.
USA	*Field Manual 3-0, Operations*. Headquarters, Department of the Army, Washington, D.C, Army Publishing Directorate. October 2022
USA	REILLY, Jeffrey M. *Operational design: distilling clarity from complexity for decisive action* Air Force Research Institute, Maxwell Air Force Base, Alabama, USA. 2012. ISBN 978-1-58566-221-0

USA	*FY19-21 Accomplishments and Investment Plan*. Army News Service. March 6, 2020.
USA	LUNDY, Michael D. *The U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045 Versatile, Agile, and Lethal*. 2018-09-01. U.S. Army Combined Arms Center (USACAC). 2018.
USA	*The U.S. Army in Multi-Domain Operations 2028.* US TRADOC Pamphlet 525-3-1. 2018.
USA	PERKINS, David G. *Multi-Domain Battle - Driving Change to Win in the Future*. Military Review. US TRADOC. 2017.
UK	*Joint Concept Note 1/20of Multi-Domain Integration*. Development, Concepts and Doctrine Centre. UK Ministry of Defence: London, UK. 2020
France	GROS, Philippe. (ed.) *Intégration multimilieux / multichamps : enjeux, opportunités et risques à horizon 2035*. Rapport n° 35/FRS/M2MC. Fondation pour la Recherche Strtégique. France: Paris. 2022.
France	CESA (ed.). *Opérations multi-milieux / multi-champs*. Centre d'études stratégiques aérospatiales. Paris: France. 2021.
Italy	MINISTERO DELLA DIFESA (ed.). *Multi-Domain Operations - Approccio Concettuale* Stato Maggiore della Difesa. Rome: Italy. 2020.
Italy	ZACCHEI, Alessandro. *Prospettive del ruolo del Potere Aereo e Spaziale sulle sfide poste dalle future operazioni multidominio.* AP-SMA-03. Centro Militare di Studi Strategici. 2021. ISBN 978-88-31203-57-9

2   DEFINING THE OPERATIONAL DOMAIN AND MULTI-DOMAIN

Referring to the above-mentioned facts, modern multi-domain operations will consist of integrating and combining the effects of all domains, as illustrated in Figure 1, in joint operations at the strategic, operational and tactical levels with an accelerated decision-making process, in order to surprise, eliminate or destroy the adversary. This rather draft definition refers to the principles of military strategy where to defeat a powerful or well-defended adversary without losing one's own forces, it is essential to use the most effective effects of each weapon or force component (land, air, navy, special operation forces) and to know how to combine them between them, at the lowest possible human and material cost, and by concealing its intentions for as long as possible. Whoever has the fastest dynamics of decisions and actions on the maximum combined effects then has a military advantage: surprise.
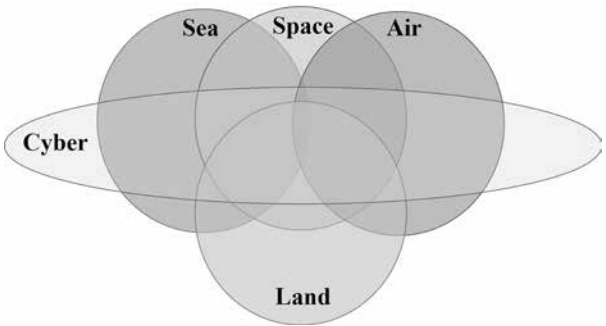
Figure 1: Elements of the Multi-Domain Operations Concept

2.1.   Dissection of Operational Domains

Although all domains of operations present different characteristics, they are strongly linked to each other. The three classic domains (land, sea and air), traditionally linked to the individual components, have more or less precise demarcation and areas of over-lapping conjunction (e.g. littoral and coastal areas between land and sea domains, aerial platforms of the land and sea components which operate in the aerial domain, aerial platforms that generate effects on the surface, etc.). The space domain is global and autonomous but at the same time, it enables the classical domains to enhance critical functions such as satellite communications and geo-positioning, navigation and timing systems. Finally, the cyber domain is characterized by its virtual and ubiquitous connota-tion and is transversal to all other domains.

While dissecting all domains, there is the apparent intersection between cyber, space and other domains/environments, as:

- space represents a domain in which discrete activities are developed that have a constant relationship with the other physical domains. Among these, those of space control have a strategic value and involve a high stake in terms of deterrence;
- activities in/through the cyber domain and the electromagnetic environment, ai-med at securing an operational advantage by inhibiting and/or degrading the ad-versary's use of the electromagnetic spectrum and cyberspace, are enabling and cross-cutting to other domains due to the spread of digital technology and the difficulty of detecting threats;
- the information environment, understood as the place where information is recei-ved, transformed, processed and transmitted, is characterized by great complexity and dynamism, as it extends beyond the physical boundaries of the crisis/conflict area and involves all the elements of national and transnational systems capable of producing effects in the general spectrum;
- increasing determination also in increasingly complicated operational areas, such as highly urbanized zones and megacities, in which military actions at various le-vels must be able to influence the operational environment to modify opponent behaviour in the desired way, at the tactical, operational and strategic level. In such contexts, all the factors that contribute to increasing the complexity of the opera-tional environment are compressed into a limited geographical area characterized by a very high civilian presence. Thus, effects in the physical dimension (such as the destruction caused by classic combat) can have exponential effects on the co-gnitive dimension.

Once the essential elements of the multi-domain operations have been traced, it is deemed necessary to frame them, at a conceptual level, and to define their main cha-racteristics and new elements.
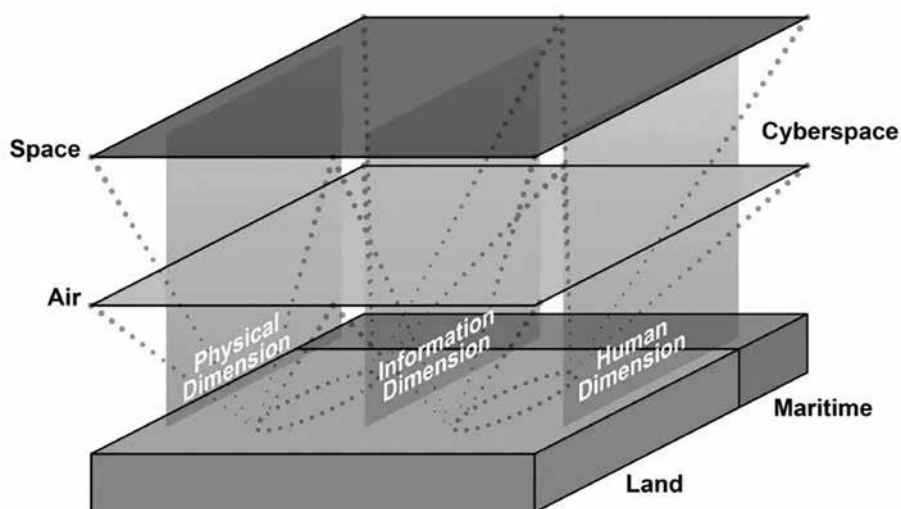
2.2   Operational Dimensions

Starting from the relationships between the domains, the actions are planned and carried out having clear dimensions to influence or in which to bring about the desired effects for the achievement of operation objectives. This can be accomplished in the following types of dimensions:[2]

- -   Physical dimension, where physical activities and physical effects occur through the interaction between geography, infrastructure, flora and fauna, individuals, states, cultures and societies; this dimension has been shaped by man over time and can only be further manipulated with considerable effort that requires time and energy;
- -   Information dimension, where intangible activities are carried out by intangible entities that can be virtual (as in the case of social media) or concrete software; this dimension can be manipulated because it is artificially created;
- -   Human (Cognitive) dimension, related to the sphere of perception and decision-making, in which social and psychological effects can be achieved, which influence the behaviour of the individual and thus achieve a lasting result.

A generic scheme that allows the evaluation of the effects to be achieved by military operations on the battlefield in three dimensions - physical, information and human - is depicted in Figure 2. Some critics nonetheless suggest that the traditional approach to military operations requires keeping the traditional physical dimension and that the military engagement in these information and cognitive dimensions is not the armed forces´ business. Analytical studies of contemporary strategic thinking seem to suggest that there are still good reasons to keep the classic construct of four physical operational domains. However, in contemporary conflicts, there is a constantly increasing need to control the interaction among these dimensions. Thus, close interaction among "*the physical, information, and human dimensions reinforces the Clausewitzian idea that war is an act of force to compel the enemy's will. In other words, physical action can influence human perceptions, behaviour, and decision-making. Although there are new capabilities in space and cyberspace, Armed forces use them just as they employ any other capability....*".[3]

---

[2] *Field Manual 3-0, Operations*. Headquarters, Department of the Army, Washington, D.C, Army Publishing Directorate. October 2022. Available on the website at https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

[3]   Ibid. p .ix.

Figure 2: Schematic diagram of operational domains and dimensions [4]

2.3   Multi-Domain Operations and Applicability of Principles of War

A comparative reading of the definition and the principle of military strategy clearly shows that multi-domain combat or operation is not a completely new principle. This approach has been noted several times throughout the ages by some of the eminent military strategists. Nevertheless, the novelty comes, on the one hand, from the appearance of the new fields of confrontation that are information, cybernetics and space and, on the other hand, from the way of integrating their effects in a dynamic way in operations conducted on land, sea or in the air.

For centuries, many military organisations subscribed to the idea that there exists a set of guiding principles or ideas that guide the conduct and study of war. These guiding principles are known as the Principles of War. There has never been universal agreement on one common list of principles.[5] As the traditional principles of war are reviewed, some will be reaffirmed, others updated and a few may be discarded or replaced. In the process, there will be new thinking about the principles that will influence doctrine and guide the transformation of 21st century forces. The objective should be clear

---

[4]   According to Field Manual 3-0, Operations

[5]   MALLICK, P. K. *Principles of War: Time for Relook*. Centre for Land Warfare Studies (CLAWS),   New   Delhi.   2009.   p.   5.   Available   at: https://www.researchgate.net/publication/344737409_PRINCIPLES_OF_WAR_-TIME_FOR_RE-LOOK

-- it is not to replace one set of principles, hostage to time and place, with another set equally constrained. There will be certainly no perfect or simple answers to the question of what depends on success in multi-domain operations. In general terms, success in multi-domain operations depends on the integration of all the factors involved, such as continuous technological development, available capabilities etc. and the ability to pick up indicators of threats to national or collective security. However, this does not mean that there should be a need for a fundamental transformation, or even a denial of the generally accepted principles of war. It is more than obvious that even in the case of multi-domain operations, Clausewitz's theory is to be applied, according to which one of the main strategic objectives is "*to conquer and destroy the main armed power of the enemy and take possession of enemy material and other sources of strength, and direct subsequent operations against places where most of these sources are concentrated.*"[6]

The concept associated with multi-domain operations, therefore, overcomes and develops the current military doctrine of joint operations, relying instead on the synergistic effect derived from the coordinated development of operations conducted in the conventional, cyber and space domains, which also extend to information and electromagnetic, and the ability to produce effects in all three dimensions (physical, virtual and cognitive). A perfect integration of all elements in the field is almost impossible to achieve, to avoid premature exhaustion of all available resources. Rather than total integration, multi-domain synchronization is used to maintain strategic advantage and initiative over an adversary. Therefore, there is a need to evolve the current concept of joint and combined operations towards a new cross-domain paradigm, even in light of the extraordinary evolution of technologies used in decision-making processes, sensors and weapon systems.

Undoubtedly, there will be a need to modify conceptual foundations for planning, and conduct of multi-domain operations due to various factors including changes in technology, geopolitical considerations, evolving threat landscapes, and shifts in military doctrine. As these factors evolve, it becomes important to adapt and update the conceptual foundations to effectively address the challenges posed by multi-domain operations. Nevertheless, the key question is, as well, to what extent there will be a need to modify the toolset, currently used for conducting comprehensive operations planning, with all respective phases and steps during which the appropriate centre of gravity is identified, design of operation is conceived, including, objectives, decisive conditions, desired effects and actions to be taken so as to achieve expected end-states. Therefore, the conceptual framework for conceiving the operational design and the subsequent executive plan will not have a significantly different form than the current one. As mentioned in the analytical study on Operational Design by Jeffrey REILLY: "*...different operational contexts require distinctive methodological approaches that distil clarity for commanders and staffs. Regardless of the operational context, operational design's effectiveness*

---

6 CLAUSEWITZ, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ: Princeton University, USA. Press, 1989.

revolves around linking design to decision-making and risk analysis. In the future, plan-ning, decision, and execution cycles will be significantly compressed."[7]

In this sense, a new methodological framework will have to be developed that can give greater incentive to the activities described by implementing integration at the joint level, more than it already is, to allow the military instrument to operate synchronous-ly in physical and virtual contexts different and with short notice times. The need to prevent and manage the escalation of competition and influence the environment and the actors who operate in it requires an approach that allows for integrated and, where necessary, preventive use of all those capacities that can help generate lasting effects in the cognitive dimension. In this context, multi-domain operations follow a sinusoidal trend (increase-decrease proportion) which differs substantially from the linear esca-lation model. Therefore, the defence will have to develop an approach that makes it possible to use, in integrated matters, all its capabilities (kinetic and non-kinetic) to en-sure its contribution to the national strategy, including through an enhancement of its non-kinetic capabilities to contribute to generating effects, also through the information environment, in the cognitive dimension.

However, the specificity of the new domains, and the extent of the resources, includ-ing financial ones, necessary to develop new capabilities require a top-down approach that allows a rationalization of the ability to define the objectives and, consequently, distribute the necessary means. This will not involve, at least in the short term, the es-tablishment of new dedicated forces, but rather the exploitation of existing excellence to overcome the single service logic and develop strategic capabilities to be integrated from the beginning at a joint level.

3 THE MODERN CONCEPTUALISATION OF MULTI-DOMAIN OPERATIONS

As far as the respective domains are concerned, it is of note that the physical domains, i.e. land, air, sea, and space, are generally well perceivable, from a military perspective. But the non-physical areas - cyberspace, and the information environment, these ones are much more difficult to be appropriately framed within a constructive definition. In fact, since its first conceptualization, a wide debate was initiated with a view to concep-tualising different approaches to this topic.

---

[7] REILLY, Jeffrey M. *Operational design: distilling clarity from complexity for decisive action* Air Force Research Institute, Maxwell Air Force Base, Alabama, USA. 2012. ISBN 978-1-58566-221-0. Available at: https://www.airuniversity.af.edu/AUPress/Display/Article/1533161/operational-design/

3.1   The Convergence of National and NATO Concepts

The initial conceptualization of the multi-domain approach, as a new concept of military operations, originates from the US military-focused model which brings a complex perspective of joint operations in all domains. Recently published Field Manual FM 3-0 Operations[8] specifies the US Army's overarching viewpoint of multidomain operations. The manual specifically emphasizes large-scale combat operations and explores their interconnection with the complete spectrum of military operations that facilitate joint campaigning, as Figure 3 schematically illustrates.
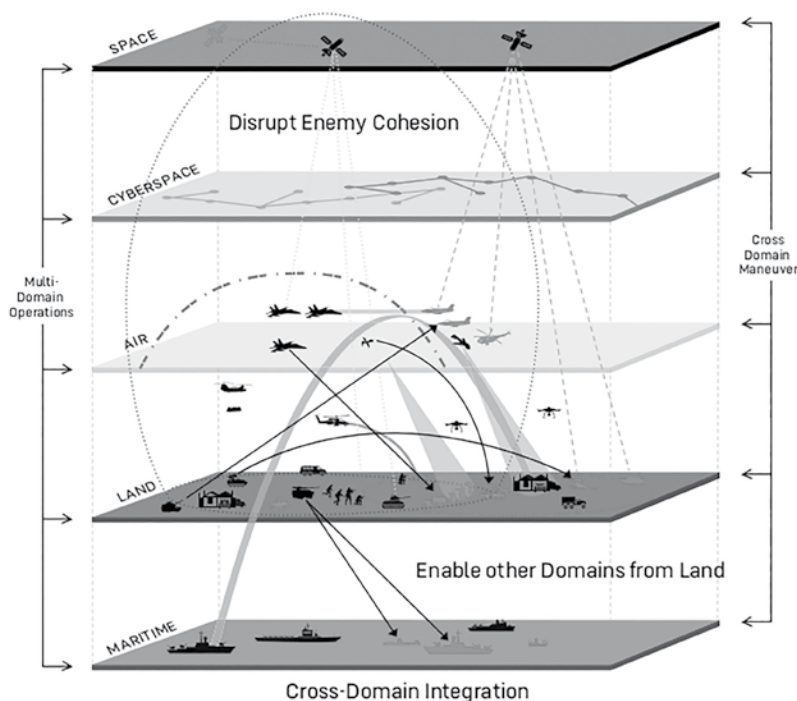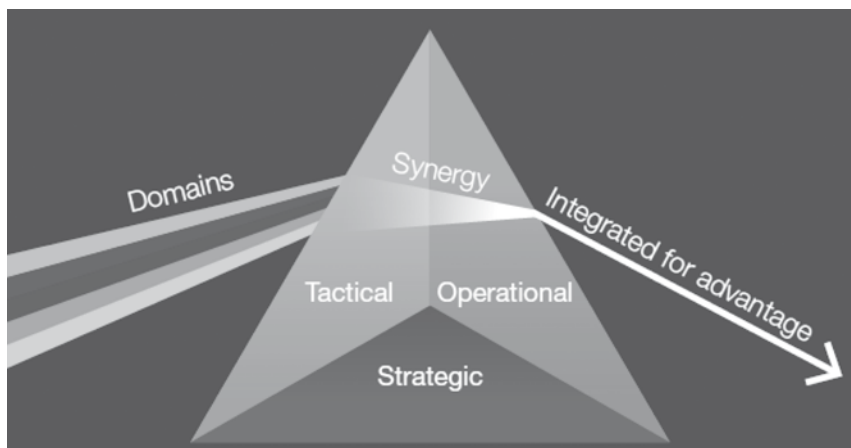

Figure 3: Multidomain operation and cross-domain integration [9]

---

8 *Field Manual 3-0, Operations*. Headquarters, Department of the Army, Washington, D.C, Army Publishing Directorate. October 2022. Available on the website at https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

9 *FY19-21 Accomplishments and Investment Plan*. Army News Service. March 6, 2020. p. 6. Available at. https://www.army.mil/article/233557/army_budgets_target_transformational_change

The manual offers comprehensive guidance on the planning, preparation, execution, and assessment of operations conducted by Army forces. It lays the foundation for integrating military power with the capabilities of other military services and joint partners, promoting effective synchronization and coordination. This vision was then joined by those who sought to integrate military instruments of power with other instruments of power. An example is the British approach with the Joint Concept of Multi-Domain Integration[10], which focuses on how to integrate all domains and levels of warfare and provides a vision for the development of an integrated force out to 2030 and beyond. Being integrated across all five domains – maritime, land, air, space, and cyber and electromagnetic – and at every level of warfare will significantly change the way of conducting military operations and the way of capability development. The configuration of multi-domain integration resulting in readiness for cross-domain synergy within operating environments through integrating and synchronising joint functions is illustrated in Figure 4.

Figure 4: Representation of multi-domain integration [11]

At the NATO level to date, there is no commonly agreed definition of multi-domain operations even if the Allied Command for Transformation (ACT) has received the task of developing the theme within the Warfare Development Imperatives descendants from the NATO Warfighting Capstone Concept, providing for the development of an initial

---

[10]*Joint Concept Note 1/20of Multi-Domain Integration*. Development, Concepts and Doctrine Centre. UK Ministry of Defence: London, UK. 2020. 90 p. Available at: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120

[11]J*oint Concept Note 1/20of Multi-Domain Integration*. Development, Concepts and Doctrine Centre. UK Ministry of Defence: London, UK. 2020. p. 11. Available at: https://www.gov.uk/government/publications/multi-domain-integration-jcn-120

Multi-Domain Operations Concept by 2022. The current draft definition[12] summarizes multi-domain operations as:

Orchestrate and synchronize military and non-military activities across all domains and environment that enable Commanders to deliver converging effects.

There is also a rather large discussion as far as the term operational domain to be used as a reference for activities related to the defence and operations planning with the Alliance. According to the Joint Air Power Competence Centre (JAPCC)[13], the proposal is to apply the working definition recognised for cyberspace at the Warsaw Summit in 2016[14]: *Operational Domain is a unique area of territory or interest in which a military force can execute joint functions (intelligence, information, command and control, fires, movement and manoeuvre, protection, and sustainment)6 in pursuit of mission accomplishment. Operational domains can be further divided into operational environments, which are subsets which require special (although not wholly unique) considerations (e.g., land is an operational domain, with forest and desert operational environments).* It should also be noted that the Allied Command for Transformation (ACT) supports various conceptual development initiatives on the subject within the Multinational Capability Development Campaign with the support of the Joint Air Power Competence Centre (JAPCC) for the development of a project on the Joint All Domains Operation - JADO.[15]

Nevertheless, while NATO has not yet published a comprehensive definition for the term domain[16] within the AAP-06 NATO Glossary of Terms and Definitions[17], it does have a definition for the operating environment which seems to be used interchangeably with the domain in numerous NATO publications. The approach and respective doctrines of multi-domain operations, as previously developed for the US Army, have been also implemented by NATO and a similar concept is being studied as well in some Alliance nations, such as the United Kingdom, France, Italy or Germany. As is the case of the US approach, NATO´s multi-domain approach is intended to combine all feasible actions to produce expected effects in all five domains of operations. It should also be noted that the Allied Command Transformation (ACT) is supporting a different conceptual development on this topic. ACT in collaboration with Joint Air Power Competence Centre (JAPCC)

---

[12]Based on outcomes of the Alliance Warfare Development Conference held from 7 to 9 December 2021. The 2021 conference was aimed at directing the process of building consensus around Multi-Domain Operations.

[13]HEREN, Henry. *Multi-Domain Operations: Inconceivable!* The Journal of the JAPCC, Edition 29, Winter 2019 /2020. Kalkar, Germany. p. 50. Available at: https://www.japcc.org/articles/multi-domain-operations-inconceivable/

[14]NATO Warsaw Summit Communique, 9 Jul. 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, '… recognise cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land, and at sea.'

[15]*All-Domain Operations in a Combined Environment*. Multi-Domain Operations. The Journal of the JAPCC. 2021. Kalkar, Germany. Available at: https://www.japcc.org/flyers/all-domain-operations-in-a-combined-environment/

[16] It is expected that a forthcoming AAP-06 edition might bring a definition of the operational domain.

[17]NATO STANDARDIZATION OFFICE (ed.). *AAP - 06 NATO Glossary of Terms and Definitions (English and French)*. NATO Standardization Office: Brussel, Belgium, 2021

in Kalkar, Germany, and NATO Joint Warfare Centre in Stavanger, Norway, recently initiated some projects to study relevant aspects of the multi-domain approach to operations.

3.2   The EU Approach to Multi-Domain Operations

When it comes to the Common Security and Defence Policy and the EU's approach to the issue of multi-domain operations, there is a noticeable difference from NATO's approach. Although the EU approach to CSDP operations is not strictly linked to the multi-domain concept, the EU is also concerned with the use of military and non-military instruments in dealing with security issues in respective operational domains. In accordance with the Strategic Compass[18], the EU should develop those military capabilities which are necessary for providing secured access and freedom of act in all operational domains. Besides that, the EU should develop a specific rapid deployment capacity as a multinational toolbox consisting of high-readiness military land, air, sea and special operation force modules for specific missions in respective operational domains.[19]

However, a potential engagement of this capacity in multi-domain operations is not yet conceptualized. In this context, the ambition of the EU is not to comprehensively cover military engagements in all operational domains, as is the case of the Alliance. Nevertheless, the conceptual model is expected to constitute an important element both for operational as well as for strategic thinking at the EU and NATO level which is highly needed. It will complement ongoing efforts and existing policy initiatives as well as provide an ex-post raison d'être based on scientific evidence. In addition, it will facilitate a common understanding and raise the awareness of the relevant authorities on the issue of hybrid threats.[20]

4   MILITARY PERSPECTIVES OF MULTI-DOMAIN OPERATIONS

Operating in a highly complex operating environment requires the armed forces to apply modern approaches. The hybrid threat, disinformation campaigns, conflicts of varying intensity and dealing with the consequences of crises (natural disasters, industrial accidents, terrorist attacks, pandemics, etc.) that characterize the development

---

[18]COUNCIL OF THE EU (ed.). *A Strategic Compass for Security and Defence - For a European Union that protects its citizens, values and interests and contributes to international peace and security*. General Secretariat of the Council, 7371/22. Belgium, Brussels, 21 March 2022

[19]MEYER Christoph, Ton VAN OSCH, Yf REYKERS. T*he EU Rapid Deployment Capacity: This time, it's for real?* Policy Department for External Relations Directorate, General for External Policies of the Union. PE 702.568 - October 2022. Belgium: Brussels. p. 13.

[20]CULLEN, P. and Coll. *The landscape of Hybrid Threats: A Conceptual* Model (Public Version), EUR 30585 EN, Publications Office of the EU, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC123305

trajectories of the future will require integrated, timely and synergistic responses, especially in the highly globalized world. *Recently, as a result of Russian aggression against Ukraine, there has been a further deteriorating of the security environment, which confirms the long-term trend in dynamic transformation of this environment, characterized by its intricacy including a whole range of aspects leading to increasing instability and uncertainty. The existence of a significant number of nuclear weapons represents a serious global threat consisting mainly of the permanent risk of their accidental or unauthorized use.*[21] In order to understand environmental threats while managing effective and timely responses capable of generating stable real-time effects in both physical and virtual operational domains, the armed forces must have the capabilities to ensure harmonization and synchronization of actions and effects. However, it is not possible to generate concrete multi-domain defence capabilities without a decisive and coordinated acceleration of the already ongoing process of integration of capabilities that are inevitably destined to be overcome and included in the very concept of multi-domain operations.

Modern forms of threats take on a very complex character, especially if they are conducted within the framework of a combined, controlled and centralized system by a single management capable of grasping and controlling the overall effectiveness of actions. Under these circumstances, an attack on a country's vital interests can be carried out by a variety of means (not necessarily weapons systems) and actors (combatants and non-combatants) while keeping the confrontation below the threshold of aggression. The conflict in Ukraine only proves the specificity of current security threats and the significant differentiation of perspectives concerning the concept of war by various subjects of international relations. For defence matter experts, Russia's aggression in Ukraine should be an opportunity to study and reflect on the nature and character of war. "*Whether the term "special military operation" or war is chosen, it's important to monitor its development, intensity, course, engaged assets, and the objectives of the parties in conflict and other actors directly or indirectly involved in the conflict. For some, the events in Ukraine might appear as combat operations of variable intensity, while for others, they might be seen as a regular war.*"[22]

The ambiguity and ubiquity of this form of aggression, together with the difficulty of identifying the aggressor himself, prevents a clear and timely recognition of an attack,

---

[21] TICHÝ, Aleš a Richard SAIBERT. *Possibilities of Developing Medical Support Capabilities in the Area of Chemical, Biological Radiological and Nuclear Defence*. Czech Military Review. 2023, 32 (1), 098-117. ISSN 1210-3292 (print), 2336-2995 (on-line). p. 99. Available at: www.vojenskerozhledy.cz. The original text in Czech is: *V nedávné době došlo v důsledku ruské agrese na Ukrajině k další akceleraci proměny bezpečnostního prostředí, která potvrzuje dlouhodobý trend dynamické transformace tohoto prostředí, charakterizovaného jeho komplexností zahrnující celou řadu aspektů vedoucích ke zvyšující se nestabilitě a nejistotě. Existence značného množství jaderných zbraní představuje vážnou globální hrozbu spočívající zejména v trvalém riziku jejich náhodného nebo neoprávněného použití.*

[22] GALBA, Jaroslav a Ján SPIŠÁK. *A Special Military Operation in the Context of Russia's Interpretation*. Czech Military Review. 2023, 32 (1), 050-068. ISSN 1210-3292 (print), 2336-2995 (on-line).p. 67. Available at: www.vojenskerozhledy.cz. The original text in Czech is: *Ať již je zvolen pojem „speciální vojenská operace" nebo válka, důležité je sledovat její vývoj, intenzitu, průběh, použité prostředky a cíle bojujících stran a dalších aktérů přímo či nepřímo zapojených do konfliktu. Pro někoho se události na Ukrajině mohou jevit jako bojové operace různé intenzity, pro druhého jako skutečná válka.*

especially if it is directed at seemingly unrelated targets, thereby exposing it to the risk of being delayed or ineffective.

Thus, there is a need to analyse how a national military instrument can guarantee the defence of the country and national interests, as well as contribute to international security. Continuity of competition requires variable synergy between the above tools in a shared and balanced effort to reduce the risk of kinetic-type collision. A military tool must always act with a different specific weight depending on the moment, even below the threshold, as it happens for example in the framework of NATO's military presence in the east of the Alliance[23], where it contributes to the generation of effects not only in the physical dimension but also in the cognitive and virtual.

4.1   Cross-Domain Cohesion and Capability Development

The distinction between operational domains should be seen as a pivotal tool for capability development, defence planning, and last but not least, for planning and conducting military operations. However, this classification does not take into consideration the entire spectrum of capabilities which shall be available to every single component of forces and the possibility of generating effects in respective domains within actions undertaken by joint task forces. Capability development in this regard should further promote interaction between relevant forces and services in all areas and optimize their organization and equipment. In principle, capability development should seek to leverage the effectiveness of individual forces operating in their respective domains and the potential for cross-domain effects.

Cross-domain actions represent the integrated combination of capabilities (military and otherwise) in the different domains aimed at exploiting a limited window of superiority and engaging the adversary in the physical, cognitive and/or virtual dimensions. To ensure the achievement of strategic objectives, cross-domain actions necessarily presuppose the synchronization of effects at different levels (strategic, operational and tactical) and the synergistic use of capabilities (kinetic and non-kinetic) across the various domains and electromagnetic environments and informative. Therefore, the purpose of cross-domain actions is to create integrated effects in the physical, virtual and cognitive dimensions, saturating the opponent. The synchronization of the effects, on the other hand, concerns the integration of activities/events over time to reach a favourable operational tempo compared to what is developed by a potential adversary, in other words, the speed and intensity of one party's actions compared to the speed and intensity of other events taking place in the operating environment. Therefore, synchronization pertains not only to the coordination of military activities at a tactical, operational and

---

[23] An important component of NATO's deterrence strategy in the eastern part of Alliance territory. In recent years, Alliance has enhanced NATO's forward presence by deploying multinational battlegroups over NATO's eastern flank, from the Baltic Sea in the north to the Black Sea in the south. These actions are to demonstrate NATO´s resolve and readiness to defend Alliance territory and populations.

strategic level but also to the necessary integration with the activities underlying the other instruments of national power in a given time interval.

Special attention should be paid to capabilities related to the cyber and space domains, which, due to their transversal nature and in line with the specific skills of the armed forces, must be carefully shaped for:

- decentralization of capability packages to individual forces to guarantee them operational autonomy and freedom of movement in their own cross-domain action;

- centralize the strategic capabilities that will have them and use them in compliance with the strategic plan and the need to synchronize effects.

In this sense, it is first necessary to define the chain of command and control for multi-domain operations in which it is necessary to identify the functional command and control structure for the decentralized conducting of cross-domain actions.

4.2   Actions and required effects in respective operational dimensions

A multi-domain environment is not a simple sum of individual domains and therefore individual capabilities. In this new perspective, the boundaries between domains blur and acquire a unity within which it is necessary to harmonize the instruments of military power and organize the actions of different capabilities to achieve multi-dimensional effects. Specifically, domains of operations are seen as one interconnected context in which the synchronized execution of actions and modulation of effort enables the achievement of a larger-scale outcome than the vision of a single domain. Based on the objectives to be achieved, the effects to be achieved are determined by influencing the actors of the reference operational environment in several dimensions, the effects being the result of actions/activities carried out by the capabilities available in different domains (including the electromagnetic and information environment). These actions, thanks to the permeability of domains and the characteristics of the information environment, can be further amplified.

In this perspective, it is necessary to note how the perception and behaviour of the actors change in order to influence them at the right time with a series of kinetic or non-kinetic actions that produce effects in physical, information and human dimensions that are related to each other. Given these assumptions, a multi-domain operations approach must allow overcoming the vertical and physical separation of individual components by exploring and improving the understanding and use of different capabilities/resources (military and civilian) to develop simultaneously multiple converging actions and produce multiple effects in multiple dimensions. Repetition of this posture over time, combined with surprise and deceptive activities, will enable control and retention of the initiative, forcing the adversary to adopt a cautious and defensive posture in all areas and dimensions.

A multi-domain environment is not a simple sum of individual domains and therefore individual capacities. In this new perspective, the boundaries between domains blur and acquire a unity within which it is necessary to harmonize the instruments of national power and organize the actions of different capacities to achieve multi-dimensional

effects. Specifically, domains of operations are seen as one interconnected context in which the synchronized execution and modulation of effort enables the achievement of a larger-scale outcome than the vision of a single domain. Based on the objectives to be achieved, the effects to be achieved are determined by influencing the actors of the reference operational environment in several dimensions, the effects being the result of actions/activities carried out by the capabilities available in different domains (including the electromagnetic and information environment). These actions, thanks to the permeability of domains and the characteristics of the information environment, can be further amplified. Planning, preparing and conducting a joint military operation, therefore, requires consideration of the relationship between joint functions and capabilities related to objectives to be achieved in respective domains.[24]

Joint functions provide a framework that enables headquarters and units to focus military capabilities at the most appropriate place and time and effectively conduct operations in the continuum of competition (at any level of intensity), ensuring force protection and sustainment. Achieving effects in the physical, cognitive and virtual dimensions is done through the synchronization and harmonization of four common actions that generate effects (manoeuvre, fires, information, CIMIC) under the directing action of the command and control structures.

CONCLUSIONS

In future operations, military superiority might be achieved by joint forces capable of carrying out missions aimed at affecting the will of the adversary through a combination of so-called multi-domain effects. These multi-domain operations are not simply a set of manoeuvres conducted in respective domains with the support of capabilities dedicated to action in another domain, e.g. an air campaign supported by assets on land, at sea, or in space and cyberspace. They must thus create offensive and defensive actions in all domains and at a pace to which the opponent cannot adequately react. Experimentation to analyse and assess whether future multi-domain operations will work is indeed essential. This effort should begin with a reasoned set of required capabilities emerging from the defence planning process. The new paradigm of multi-domain operations must be based on the development of a unified and shared national strategic vision that clearly defines the political, economic and legal framework within which such operations can be conducted and clearly identifies the areas of national interest that must be protected. There is also a strong need for a government institution that defines the national security strategy with a view to coordinate, integrate and synchronise the tools of national power (diplomatic, informational, military and economic) for crisis management and

---

[24] NATO and U.S. joint doctrine were jointly worked on and coordinated with the revision of NATO AJP-3, Allied Joint Doctrine for the Conduct of Operations. According to the latest version of NATO AJP-3, 8 joint functions are command and control, manoeuvre, intelligence, fires, sustainment, information, protection, and CIMIC.

international competition in a multi-domain context. On the other hand, at the operational level, it undoubtedly seems necessary to define the optimal configuration of a command and control model that goes beyond the logic of sectoral competencies and can provide coherence to the various information supplied by peripheral sensors, allowing for the integration of different situations into a single, coherent and updated general situation - of a multi-disciplinary common picture - on the basis of which decisions will be made.

A further key element of multi-domain operations will be the continuous search for integration and interoperability between systems, processes and actors involved in the various domains, both at national and international/supranational level. Finally, it will be crucial to define the new role of the human dimension in the evolution of its relationship with emerging technologies, with particular reference to artificial intelligence. In this sense, the renewal of the process of selection, training and growth of human capital will be strategic and must be oriented both to the development of skills with a technical-specialist connotation and to the education of leaders to deal with different realities and to use new tools available. In this reference framework, therefore, the defence intends to promote a collective debate on what could be the general guidelines to allow the development of a national approach to multi-domain operations and, specifically, the guidelines for the defence capable of outlining the main transformation and innovation needs of the military instrument. It should be noted that a comprehensive approach to multi-domain operations requires more detailed analyses. However, current knowledge and experience show important advances in predicting the modern warfighting concept. This concept is also ground-breaking in that it tries to establish synergy and convergence between so far individual and isolated domains. However, more work remains to be done to answer the question of to what extent an approach to multi-domain operations is necessary to be implemented and how future joint forces will cooperate in such an operating environment in order to achieve the expected military end-state. This is a key question that needs to be answered to transform the concept into doctrine and theory into practice.

Author: ***Zdeněk Petráš, PhD. (Colonel ret.)*** *born in 1964, in 1989 graduated from the Military College of Land Forces in Vyskov (CZE). In 2008, he completed master´s degree at the Université Panthéon-Assas Paris, in defence industry dynamics. In 2016, he obtained PhD. degree in economics and management program at the University of Defence Brno (CZE), specialising in military capability assessment. After several years spent as a staff officer at the General Staff of the Czech Forces and in NATO and EU military structures, he currently works as a researcher-fellow at the Centre for Security and Military Strategic Studies. He is systematically engaged in issues related to defence planning and he is an author of a few articles and publications dealing with this topic.*