

MULTI-DOMAIN OPERATIONS IN A BRITTLE, ANXIOUS, NONLINEAR AND INCOMPREHENSIBLE WORLD

Octavian-Grigore NEȘTIUT, Vlăduț-Constantin BERBUNSCHI

Headquarters Multinational Corps South-East, Sibiu, Romania
octavian.nestiut@gmail.com, berbunschivladut@yahoo.com

Abstract: *The current era, characterized by brittleness, anxiety, nonlinearity and incomprehensibility (BANI), represents an environment in which the military operations must be planned, conducted and adapted in a comprehensive approach using all resources from all the domains that can be employed in order to achieve the desired end state. To become or remain relevant, the military organizations must achieve the state in which they are capable of mobilizing the proper resources from all domains and utilizing them wisely in order to create converging effects at a speed of relevance. The Multi Domain Operations (MDO) military concept is developed for neutralizing peer or near peer adversaries, having as its core idea the integration of armed forces from all five domains (land, air, maritime, space and cyberspace) that generates a relative superiority which creates deterrence leading to strategic achievements without using just conventional military operations. It represents a pragmatic manifestation of the holistic approach: the whole is more than the sum of its own parts. A successful implementation of MDO enables the military instrument of power to plan, prepare, orchestrate, and execute actions that are synchronized, and activities in close collaboration with other instruments of power, relevant actors and stakeholders across all domains and environments at a scale and speed that will outpace the adversary. A successful approach will deliver tailored options in the right time and at the right place, building a relevant advantage in shaping, and fighting, and creating new dilemmas that can influence in a decisively way the attitudes and behaviors of the adversaries and relevant audiences.*

Keywords: military organization, multi domain operations, military instrument, converging effects, relevant audience.

1. Conceptual determinations regarding BANI world that we live in and MDO

Born in the late 1980s after the Cold War, the concept that was used to framework the world was VUCA, which stands for Volatile, Uncertain, Complex and Ambiguous [1].

However, due to the fact that nothing is permanent, in 2018 a new concept was brought into the spot light by the futurist Jamais Cascio. The new concept is BANI: Brittle, Anxious, Nonlinear and Incomprehensible, a concept that is reflecting with high accuracy the new reality [2].

B stands for Brittle – the modern systems, structures and supply chains on which our day-by-day life depends are shockingly fragile.

A is for anxious – constant uncertainty that creates a sense of fear and helplessness, making it difficult to make decisions.

N is for Nonlinear – an event eventually triggers other events that are completely unforeseen. So, careful linear thinking is now a liability. Nowadays leaders must accept the fact that the proper answer comes only from action, rapid iteration (tweaking) and agility. I stands for Incomprehensible – being smart is no longer enough when the world is incomprehensible. The current world is drowned in data, information and technology that integrates AI accelerates and acts faster than the human mind can process. In this case, the unsettling truth is that the leaders do not need to comprehend everything; the minimum required is to take calculated risks, move quickly and, the most important aspect,

lean on their intuition when the big picture cannot be seen and understood.

MDO represents the orchestration of military actions and activities that are part of an operation, across all operational domains and in all environments. Also, MDO includes the synchronization of military actions and activities with non-military activities, in order to enable the military organization to generate converging effects (cognitive, virtual, physical, etc.) at a speed of relevance. Successfully implementing Multi-Domain Operations (MDO) empowers the military to seamlessly synchronize efforts with other national instruments of power, stakeholders, and partners across all domains. By operating at superior speed and scale, the force can deliver tailored options that shape the environment, contest adversaries, and dictate terms, creating dilemmas that decisively influence the behavior of opponents and relevant audiences [3].

1.1. The problem to which MDO represents the solution

Strategic competition with China and Russia, which intensified in the mid-2010s, became increasingly apparent and raised growing doubts about the stability of the existing international order. By employing large-scale Anti-access/area-denial capabilities, smaller actors disproportionately increased the cost of intervention for stronger competitors, turning them into unsustainable endeavors. In addition to this, the technological progress brought the situation in which a traditionally uncontested domain like Space became more contested, while also creating a new and more competitive domain, Cyber.

Moreover, the increase of complexity in the information environment, which gained a more important role due to the higher manipulation opportunities offered by digital technologies, especially in democratic societies, generated a new paradigm in which the MDO Concept was created to respond to the new threats [3]. MDO is based on an intensified interaction between military organizations and nonmilitary actors such as

Diplomacy, Information and Economic levers through collaboration and synchronization. MDO concept is focused on connectivity that delivers converging effects in Land, Maritime, Air, Cyberspace, Space.

“Starting from the early 2010s, the U.S. armed forces began a phase of conceptual experimentation aimed at regaining military superiority. MDO, designed to neutralize coercion, manage escalation, and penetrate contested environments by seamlessly exploiting capabilities that belong to different domains, is at the core of these conceptual innovations” [4].

MDO attracted increasing attention and acquired increasing importance within NATO due to the fact that U.S. concepts, doctrines, and frameworks inevitably flow to NATO Allies through a mix of socialization, imitation, and competition. So, MDO became a NATO Concept.

2. Principles and enablers of NATO’s MDO Concept

MDO Concept reflects a natural way of evolution from joint operations to an approach in which the capabilities of each domain even if the resources needed and used are owned by a military organization or by a non-military provider.

NATO’s MDO Concept is based on four agreed guiding principles [5]:

- 1) Unity – allows coordinated action of all capabilities towards a common objective, requiring collaboration, transparency and trust and benefits from a willingness to bridge diverse national perspectives.
- 2) Interconnectivity – enables the exchange of data and information to build understanding. It is still challenged by differences between legacy and modern platforms and requires resilient and standardized data.
- 3) Creativity – stimulates the development of boundless opportunities. It relies on the ability to analyze situations from different perspectives and is enhanced by an ability to visualize the context.
- 4) Agility – allows the force to take advantage of fleeting opportunities. It

requires initiative, relative speed prioritization, and flexibility and a mandatory condition: the application of mission command.

The MDO concept is enabled by the following:

1. Data and Digital Transformation – the NATO Warfare Development Agenda (WDA) identifies data as a critical enabler; inadequate data sharing and tight limitations on rates of data exchange are just two of the issues that must be addressed. *“The Alliance members must connect with one another via systems with sufficient capacity to enable persistent interaction. Digital transformation efforts tend to gravitate towards technical specifications and substantial investments.”*

However, for achieving the highest aspiration of MDO it is mandatory that culture, processes, and people be included in the transformation process” [5].

2. Technological Advantage – *“MDO concept needs to be optimized through an effective exploitation of technology, which provides information and a decisive advantage. This includes the use of Emerging Disruptive Technologies (EDTs), Artificial Intelligence (AI) and the transition to a data-centric organization. Just using this, the organization will unlock opportunities to advance interconnectivity and interoperability across national forces and the other Instruments of Power”* [5].

3. Multi-Domain Command and Control (C2) – MDO relies on agile, collaborative and empowered C2. *“This requires a crossdomain understanding and asymmetrical thinking supported by a continuous and robust flux of information and communication systems. The success of future operations depends not only on the preparation, capability, and agility of forces, but also on the ability of commanders to operate in a complex environment that contains physical and non-physical domains. This requires cross-domain understanding, agile and asymmetrical way of thinking supported by robust and continuous*

information flow and communications systems” [5].

4. Education, Training, Exercising, and Experimentation – “MDO requires investments in technologically enabled training at the national and NATO levels and, of course, commanders and staff that can exploit the capabilities across the domains, based on technologically enabled understanding to generate a relative advantage” [5].

To cultivate leaders and personnel capable of operating across all combat domains (land, sea, air, space, and cyber), military institutions must synchronize professional education, tailored training, and practical operational requirements [6].

To succeed in MDO, we need versatile warfighters capable of exploiting opportunities across all operational domains. This necessitates an upgrade in collective training to include higher-complexity scenarios, surpassing the scope of traditional national training efforts.

Effective MDO experimentation goes beyond analytical and planning considerations to include training and education. Yet, addressing the cultural aspects is crucial, requiring an integrated exchange to ensure realistic and productive testing.

2.1. The Data Tenets in Relations with MDO Principles

The following four Data Tenets are focused on supporting the momentum towards NATO becoming a data-centric organization:

- Data sharing – linked to the MDO Principle of Unity, data sharing is directed towards a national willingness, commitment and dedication to make data accessible. In this case, a full commitment made by all nations is mandatory.
- Data exchange – linked to the MDO Principle of Interconnectivity, data exchange comprises the pathways and gateways that link entities to enable data sharing. In order to achieve this, a secure and resilient data exchange is needed.
- Data appreciation – linked to the MDO Principle of Creativity, data

appreciation core idea is making the most out of the data.

- Data Exploitation – linked to the MDO Principle of Agility, data exploitation provides knowledge and understanding from Big Data to support the decision-making process.

3. Cyberspace domain

The Alliance increasingly functions within a hyper-connected environment, particularly across the cyber and information domains, making seamless data transmission and network stability critical to military and civil sectors alike. Seizing upon this structural dependence, malicious actors actively seek and exploit vulnerabilities in both military and non-military information networks. These adversarial campaigns aim to compromise data integrity, steal sensitive information, and extract geopolitical or financial gains [7].

“The digital networks need to be safeguarded against information denial by disruption, manipulation, exfiltration, degradation or destruction. In an interconnected world where military success may depend as much on the ability to control one’s narrative as the ability to create physical effects, freedom of action in cyberspace may be as important as control over the other domains” [8].

Fundamentally, cyberspace is an artificially constructed, rapidly advancing computational environment. Although its operations are globally interconnected, the underlying physical infrastructure is bound by geographical borders that dictate national jurisdiction. Consequently, applying classical, geography-based operational boundaries to the cyber domain presents a significant strategic challenge [9].

“Cyberspace is not only in constant flux but, even more importantly, it may be used by anyone for almost any purpose. Cyberspace is also distinct in that its underlying physical elements are entirely man-made, which is different from the other domains. Risks in cyberspace may be managed through manipulation of the domain itself” [9]. A

cyberspace operation represents an action in or through cyberspace intended to preserve friendly freedom of action in cyberspace and/or to create effects to achieve commanders’ objectives.

There are two types of cyberspace operations:

- Defensive cyberspace Operations – actions in or through cyberspace that preserve friendly freedom of action;

- Offensive Cyberspace Operations – actions in or through cyberspace that project power to create effects that achieve military objectives.

NATO does not conduct Offensive Cyberspace Operations.

4. Space domain

Space is the volume beyond the upper limits of airspace – 80/100 km.

In December 2019, NATO leaders declared space to be the alliance’s fifth domain of operations. In 2024, the Allies activated the NATO Space Operations Centre (NSpOC) at Allied Air Command, Ramstein, Germany.

4.1. Space as war-fighting Domain *“Over 12.000 active satellites are orbiting the Earth, and over half of them are operated by NATO countries, enabling technology from mobile phone and banking services to weather forecast. Military commanders rely on space assets to navigate, communicate, share intelligence, detect missile launches and for environmental monitoring”* [10].

NATO has extended its mutual defence clause, Article 5, to cover potential attacks on or originating from space [11].

5. Conclusions

In a BANI world, MDO became a must. The strategic competition between different international actors, that are trying to employ all the resources in all domains in order to project their interests and gain influence and/or control over the contested areas or just for gaining prestige, generated a new paradigm. This paradigm comes with lots of unknown situations, vulnerabilities and potential or real threats for the existing world order. So, in order to mitigate the threats,

protect the vulnerabilities and gain and maintain the initiative, the military organizations came up with a new approach that represents the orchestration of military activities employing all necessary resources across all operational domains and environments, synchronized with nonmilitary resources and activities in order to achieve the desired end state. NATO's MDO approach integrates all military domains—land, air, maritime, cyber,

and space—with external partners to execute synchronized actions at the speed and scale required for relevance.

This approach synchronizes actions to deliver tailored, timely options that create advantages in shaping, contesting, and fighting. It presents adversaries with new dilemmas while decisively influencing the behavior of their forces and key audiences.

References

- [1] Kruse, K. Forget VUCA. The World Is BANI Now. Internet: Forbes, Feb 03, 2025. <https://www.forbes.com/sites/kevinkruse/2025/02/03/forget-vuca-bani-is-the-newframework-world/>. Accessed May, 09, 2026.
- [2] Cannon, S. The Alliance's Transition to Multi-Domain Operations, An AIRCOM perspective. Internet: JAPCC Journal Edition 37, 2024. https://www.japcc.org/wpcontent/uploads/JAPCC_J37_Art-02_screen.pdf. Accessed May, 09, 2026, p. 16.
- [3] Gilli, A., Gilli, M., Grgic, G. NATO, multi-domain operations and the future of the Atlantic Alliance. Internet: Comparative Strategy 2025, vol. 44, No. 1, 73–91. <https://www.tandfonline.com/doi/epdf/10.1080/01495933.2024.2445491?needAccess=true>. Accessed May, 09, 2026, pp. 74-75.
- [4] Internet: Nato Digital Backbone & Nato Digital Backbone Reference Architecture - Executive Summary. https://www.nato.int/content/dam/nato/legacy-wcm/media_pdf/2024/12/pdf/241213DBRA.pdf. Accessed May, 09, 2026, p. 2-11.
- [5] Cannon, S. The Alliance's Transition to Multi-Domain Operations, An AIRCOM perspective. Internet: JAPCC Journal Edition 37, 2024. https://www.japcc.org/wpcontent/uploads/JAPCC_J37_Art-02_screen.pdf. Accessed May, 09, 2026, pp. 17-20.
- [6] Wilson, C. Embracing the Future of a Multidomain Army, December 13, 2022. Internet: <https://www.armyupress.army.mil/Journals/NCOJournal/Archives/2022/December/Embracing-the-Future-of-a-Multidomain-Army/>. Accessed May, 14, 2026.
- [7] Internet: <https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence>. Accessed May, 13, 2026.
- [8] Internet: <https://www.atlanticcouncil.org/blogs/new-atlanticist/so-much-for-a-worldwithout-borders-countries-are-marking-their-territory-in-cyberspace/>. Accessed May, 10, 2026.
- [9] Allied Joint Publication-3.20. Allied Joint Doctrine for Cyberspace Operations, Edition A Version 1, January 2020, Internet: https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1.pdf. Accessed May, 10, 2026, p. 1.
- [10] NATO's approach to space. Updated: 30 July 2025. Internet: <https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-approach-to-space>. Accessed May, 10, 2026.
- [11] Lye, H. Space attacks could trigger Article 5: NATO, June 15, 2021. Internet: <https://www.army-technology.com/features/space-attacks-could-trigger-article-5nato/?cf-view&cf-closed>. Accessed May, 10, 2026.