Proceedings of 4th International Conference CNDCGS'2024
ISSN 2669-2023 (print) / ISSN 2538-8959 (on-line) / DOI 10.3849/cndcgs.2024.357

The Multi-Domain Approach to Military Operations and its Challenges to Intelligence and Intelligence, Surveillance, Reconnaissance

Ondrej KACMARIK[1*], Radovan VASICEK[1]

[1]Department of Intelligence Support, Faculty of Military Leadership, University of Defence, Kounicova 156/65, 662 10 Brno, Czech Republic

Correspondence:[*]ondrej.kacmarik@unob.cz

Abstract

This paper discusses the multi-domain approach to military operations. Through comparative research and literature review, authors analyze how Western and peer adversary countries, namely the Russian Federation and the People's Republic of China, perceive and implement multi-domain operations. The article also identifies the challenges presented by the multi-domain character of the contemporary and future operating environment to intelligence and ISR. It highlights the crucial role of timely intelligence and surveillance in the diverse and contested operating environment, emphasizing the need for new technologies like artificial intelligence and big data processing.

KEY WORDS: *multi-domain operations, North Atlantic Treaty Organisation, Russian Federation, People's Republic of China; Intelligence Surveillance Reconnaissance, threat, doctrine.*

Citation: Kacmarik, O.; Vasicek, R. (2024). The Multi-Domain Approach to Military Operations and its Challenges to Intelligence and Intelligence, Surveillance, Reconnaissance. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 11-13 September 2024. ISSN 2538-8959. DOI 10.3849/cndcgs.2024.357.

1. Introduction

Modern militaries, particularly those within the North Atlantic Treaty Organisation (NATO), have for decades used the term joint when discussing operations coordinated across multiple domains. In the context of joint operations, most military forces have been focused primarily on the physical domains of the operating environment (OE), i.e. land, maritime and air. In practice it means that until recently operations and planning staffs preferred to seek solutions in these traditional domains, and due to multiple factors, they often struggled with relatively new operational domains such as space and cyberspace, and non-physical environments, including the electromagnetic environment (EME) and information environment. As the military conflicts of the last decade have underscored the ever-growing dynamics of evolution of threats and challenges, which the coalition forces will most likely counter in the near future, a perception of the OE as a composite of separate domains is no longer acceptable.

In a multi-domain approach, these domains and environments are interconnected and interdependent, with capabilities in one domain supporting and enhancing operations in others [1, p. 3-3]. In general, it refers to a strategy that integrates capabilities and operations across the domains of the battlespace to achieve military objectives. Interestingly, during their research, the authors also encountered viewpoints suggesting that a multi-domain approach is not a novel concept. This can be exemplified by Sun-tzu's assertion: *"There are not more than five musical notes, yet the combinations of these five give rise to more melodies than can ever be heard. In battle, there are not more than two methods of attack – the direct and the indirect; yet these two in combination give rise to an endless series of maneuvers."* [2] The emergence of this concept, despite not being perceived as exactly novel by some, has nonetheless instigated significant changes and complexities in the way modern warfare is strategized and executed. Today, its influence in reshaping warfare strategies on a global scale is undeniable and its importance in the context of contemporary warfare continues to escalate.

NATO and most of its member states have been gradually considering challenges, opportunities and possibilities related to inevitable implementation of a multi-domain approach. Several concepts have been developed by various nations so far, however, they are often inconsistent or even misunderstood with regard to terminology, scope and policies [3, p. 15].

Peer-review under responsibility of General Jonas Žemaitis Miltitary Academy of Lithuania and University of Defence, Czech Republic

Despite this lack of consistency, continuous developments of our approaches towards future military operations underscore the need for detailed and comprehensive knowledge of the operating environment or synergistic effects of our targeting. Responding to challenges posed by contemporary and emerging security threats, this approach recognizes that modern conflicts are not limited to a single domain and require coordinated efforts across multiple domains to effectively project power, maintain superiority, and achieve mission success. The complexity and variability of contemporary military operations requires situational awareness about the current developments in the joint operations area and the OE, which must be shared across all command and control (C2) levels with special emphasis on the operational and tactical levels.

In this respect, intelligence is a critical joint function which significantly contributes to comprehensive understanding of the OE which is essential to identify opportunities, anticipate threats, and make informed decisions. It is a key enabler which provides the situational awareness and understanding necessary to achieve military objectives in a highly contested and interconnected battlespace.

2. Methodology and limitations

This paper employs a qualitative research approach, analyzing publicly available information, military doctrine, and strategic communications. The article firstly compares different perspectives of the most prominent proponents of a multi-domain approach, such as the United States of America (USA), the United Kingdom (UK) or NATO, with the aim to identify and clarify differing and similar aspects of the concepts explored. The comparative research was focused predominantly on the most recent doctrinal documents related to multi-domain operations (MDO) released by the abovementioned countries and organization. The authors also performed systematic a literature review in order to analyze how the Western multi-domain approach is perceived and interpreted by peer adversaries/competitors, namely the Russian Federation (RF) and the People's Republic of China (PRC), and how a multi-domain mindset is reflected in military strategies of both countries. The challenges presented by the multi-domain character of the contemporary and future OE to intelligence and intelligence, surveillance, reconnaissance (ISR) were identified through a case study of the multi-domain interrelation in the conflict in Ukraine and analysis of informal interviews conducted within the Czech Armed Forces intelligence and ISR community.

In this article, there are several limitations that should be taken into consideration when interpreting the results:

22. Limited Public Information: While some information about military operations is publicly available, much of it is often restricted or sanitized for security reasons. This limitation sometimes hinders the depth as well as broader context of the research.
23. Changing Nature of Warfare: Warfare and military strategies are constantly evolving in response to technological advancements, geopolitical shifts, and changes in tactics. Keeping up with the latest developments and trends in multi-domain operations can be challenging.
24. Limited Academic Literature: While there is increasing interest in multi-domain operations, academic literature on the topic may still be relatively limited compared to more established fields. Finding scholarly sources to support this research requires thorough searching and critical evaluation of available literature.

3. The implementation of the multi-domain approach in selected countries

The multi-domain approach recognizes that modern warfare extends beyond traditional battlefields and that victory requires superiority across all domains. The main reason for the development of the multi-domain concept was the changing nature of modern warfare, particularly the rise of near-peer competitors, advancements in technology, and the increasingly interconnected and interdependent nature of the global battlespace.

The USA, or more specifically the U. S. Army, became the main proponent of the multi-domain concept during the second decade of the 21st century. In December 2018, the U.S. TRADOC published its Pamphlet 525-3-1 "The U.S. Army in Multi-Domain Operations 2028" [4]. It explained the reasons why the USA had adopted the MDO concept claiming that *"China and Russia exploit the conditions of the operational environment to achieve their objectives the integration of diplomatic and economic actions, unconventional and information warfare (social media, false narratives, cyber-attacks), and the actual or threatened employment of conventional forces"*. [5, p. 1]

The multi-domain approach has gradually become a new paradigm to NATO member countries as well as for NATO itself. However, understanding the multi-domain concept among the USA and NATO countries presents several challenges, including differing definitions, terminology, doctrinal issues, technological solutions and requirements, security and legal aspects etc. This chapter elaborates on different perspectives regarding the multi-domain approach in order to provide the context for identification of challenges associated with intelligence and ISR.

When exploring the U.S. multi-domain approach to operations, it is important to highlight that MDO should not be simply perceived as further evolution of joint operations. In fact, in the U.S. context there are two major concepts of the multi-domain approach – the MDO and Joint All-Domain Operations (JADO). While they are similar in many respects, there are key differences between them.

MDO is a concept that has been primarily developed by the U.S. Army. Having been outlined by the aforementioned Pamphlet 525-3-1, it is doctrinally anchored in the Army's Field Manual (FM) Operations (FM-3.0) published in October 2022. The document defines MDO as *"the combined arms employment of joint and Army capabilities to create and exploit*

relative advantages to achieve objectives, defeat enemy forces, and consolidate gains on behalf of joint force" [1, Glossary – 10] while also claiming that *"all operations are multidomain operations"*. [1, p. 1-3]

The primary concept of the Army is to succeed through competition in every domain without conflict, thereby discouraging a potential enemy. If this deterrent strategy fails, the Army, in collaboration with Joint forces, aims to infiltrate enemy anti-access and area denial (A2/AD) systems to facilitate strategic and operational maneuvering of U.S. forces [5, p. 1]. MDO describe manoeuvering across these domains as convergence, with tactical commanders needing to understand how their actions shape other domains, and exploiting successes, or guarding against vulnerabilities that may emerge in them [3, p. V]. In order to obtain such understanding, tactical commanders must be able to receive relevant intelligence, therefore in October 2023, the U.S. Army published FM-2.0 Intelligence which describes in detail the role of army intelligence in MDO closely following FM 3-0: "*To provide effective and flexible intelligence support, intelligence professionals must understand multidomain operations. FM 3-0 provides many doctrinal concepts that are important to intelligence professionals."* [6, p. 2-1] The importance of intelligence to MDO is evident from the statement: "*Intelligence drives multidomain operations and multidomain operations enable intelligence"*. [6, p. xi] In this way, the U.S. Army maintains doctrinal complementarity and compatibility.

While MDO focuses on integrating U.S. Army operations across multiple domains to create advantages for friendly forces and disadvantages for adversaries with the goal to enable maneuver and operations across all domains, JADO is a broader concept that encompasses all branches of the military. Unlike MDO, it has not been doctrinally established yet, therefore it should be considered more a vision of future U.S. military operations.

The aim of JADO is to connect every sensor to every shooter in all domains to achieve decision superiority and overmatch against adversaries. It seeks to integrate capabilities across all domains, the electromagnetic spectrum, and the information environment to achieve operational objectives. It is believed that in this way, U.S. forces will be able to create multiple simultaneous dilemmas for an enemy which cannot all be solved and which compel hostile troops and commanders to make difficult or impossible trade-offs [7, p. 3]. The key is synchronizing decisions and effects across all domains in a contested battlespace [8]. This will require an accelerated decision-making process supported by a robust and timely intelligence support to ensure that all actions are integrated, synchronized and integrated at speed and scale needed to gain advantage and accomplish the mission [9, p. 9]. In other words, is a military concept that refers to a seamless integration of operations across all domains of warfare – land, air, sea, space, and cyber to achieve a more effective and efficient joint force. The goal of this concept is to ensure information and operations synchronization across these domains in real-time to outpace adversaries. This approach is seen as a way to maintain a strategic advantage and respond to threats more quickly and effectively.

A crucial enabler to JADO, and actually its tangible implication, is Joint All-Domain Command and Control (JADC2) Strategy. In March 2022, the U.S. Department of Defense (DoD) published "The Summary of the Joint All-Domain Command and Control (JADC2) Strategy" which formulated guiding principles to promote coherence of effort including information sharing capability improvements, Joint Force C2 systems resilient in degraded and contested EME, layered security features or broadly applicable common data standards [10, p. 2]. Also in March 2022, the DoD signed "The JADC2 Implementation Plan" which provides the framework and methodology to achieve the JADC2 strategy and goals [11, p. 21].

So, while both MDO and JADO seek to integrate operations across multiple domains, the key difference lies in their scope and the degree of integration. JADO represents an evolution of MDO, aiming for a fully connected and integrated joint force across all domains, however, it still sees the joint force as the pivotal stakeholder in the future military operations.

The evolution of the global security environment during the second decade of the 21st century has also initiated extensive doctrinal and organisational changes in the British Armed Forces. The British Ministry of Defence has taken a somewhat different approach to multi-domain integration than the USA, consisting of adapting the existing institutional framework to better coordinate the development and effects of emerging military capabilities [12, p. 3]. While the USA has focused on the tactical and operational challenges posed by the PRC in the South Pacific, the UK sees the aggressive foreign policy of the RF and its associated hybrid engagement, particularly in Eastern Europe, as the main threat. The British concept of the multi-domain integration (MDI) is described in the Joint Concept Note 1/20 which was published in November 2020. The core tenet of the MDI is based on the assumptions that it involves partners across the government, while the strategic objectives of the UK will be pursued through its designed alliance with NATO, emphasizing that the North Atlantic Treaty Organization remains a crucial part of this strategy [13, p. 31]. The practical implementation of the MDI concept into the intelligence doctrine was done in August 2023 when the British Ministry of Defence published the 4th edition of the Joint Doctrine Publication 2-00 Intelligence, Counter-intelligence and Security Support to Joint Operations (JDP 2-00). The document emphasizes the fact that "*information is a critical enabler to mission command and a multi-domain approach, as it enables understanding, decision-making, and command and control. The ever-increasing volume of information and data available represents one of the biggest challenges for producing intelligence and will continue to challenge available human analytical capacity".* [14, p. 20] According to JDP 2-2.00, "*MDI seeks to generate advantage through integration across the three levels of operations (tactical, operational and strategic) and the five operational domains to create multi-domain effect that adds up to far more than simply the sum of the parts. Operations spanning multiple operational domains are an evolution of joint operations, reflecting the introduction of the space, and cyber and electromagnetic domains".* [14, p. 109]

The UK MDI concept and the US MDO approach share the common goal of integrating operations across all military domains – land, sea, air, space, and cyberspace – for more effective combat operations. However, the specifics of their approaches can differ based on their unique strategic contexts, military structures, and doctrines. From the conceptual perspective, the US's MDO concept is spearheaded by the US Army and emphasizes the integration of capabilities to penetrate and disintegrate enemy A2/AD systems. The UK's MDI approach, while also aiming for operational integration, places a strong emphasis on the cooperation and interoperability with allies, particularly within the NATO framework, and it also involves

partners across the whole government spectrum to ensure a coordinated and effective response to shared threats. Concurrently, MDI may also place a greater emphasis on a broader range of operations, including counter-terrorism and peacekeeping missions, and on adversary activities across the political or information domains across the operational variables of the Political, Military, Economic, Information, Infrastructure-Physical, Time (PMESII-PT) model, thus not concentrating only on military capabilities. In addition, there are also different implications for implementation of both concepts. The USA has a larger military with vast resources, and its MDO concept involves significant restructuring and modernization of its forces. The UK, on the other hand, has a smaller military and its MDI approach may focus more on optimizing existing structures and improving coordination between different branches. Both countries recognize the importance of emerging technologies, such as artificial intelligence, machine learning, and cyber capabilities. However, the MDO concept heavily emphasizes the development and deployment of new technologies to gain an advantage in future conflicts. The MDI, while also acknowledging the role of technology, may place a greater emphasis on the integration and best use of current capabilities to improve decision-making, situational awareness, and the speed and precision of military operations.

NATO had been discussing a multi-domain approach for several years until it was formally acknowledged in the Brussels Summit Communiqué of 2021 which mentioned, among others, Russia's growing multi-domain military build-up, threats in a multi-domain environment and commitment of the Alliance to ensure a flexible, agile, and resilient multi-domain force architecture [15]. It was further developed in NATO's Strategic Concept, adopted at the NATO Summit in Madrid in June 2022. According to this document, NATO's multi-domain approach combines military and non-military tools, as well as integrates efforts across different domains to achieve strategic objectives [16]. In the NATO context, it means that MDO prepare, plan, orchestrate and execute coordinated military activities across all operating domains and environments. These actions are synchronized with non-military activities and enable the Alliance to achieve an advantage in shaping, contesting and fighting and presents dilemmas that decisively influence the attitudes and behaviours of adversaries. Thus, it essentially merges both U.S. MDO and UK MDI concepts [9, p. 10].

Despite the common tenets, it should be noted that U.S. MDO concept is premised on the U.S. needing to confront China and Russia simultaneously. European allies, however, do not necessarily see China as a competitor. Other contradicting opinions point out that the U.S. MDO has a similar focus as offensive operations in a conflict, with three main components that are clearly offensive in nature: penetrate, disintegrate, and exploit [17]. This may seem to be a contradiction to NATO primarily defensive posture. However, while the MDO has offensive components, it also emphasizes the importance of defense and deterrence which is then fully in line with NATO policy as evidenced by one of the statements from the Vilnius Summit Communiqué: "*We will individually and collectively deliver the full range of forces, capabilities, plans, resources, assets and infrastructure needed for deterrence and defence, including for high-intensity, multi-domain warfighting against nuclear-armed peer-competitors".* [18] It was the Vilnius summit in 2023 that introduced NATO's most concrete commitments, steps and measures in implementation of a multi-domain concept so far. It was stated that the Allies would be committed to fully resourcing and regularly exercising plans for high-intensity and multi-domain collective defense. A new multinational and multi-domain Allied Reaction Force will provide more options to respond swiftly to threats and crises. NATO's command and control will be strengthened to ensure agility, resilience, and adequate staffing for executing plans. This will enhance the ability to conduct exercises, manage NATO's posture in peacetime and during transitions, and undertake command and control for various missions, including large-scale MDO for collective defense. Work will continue on MDO, enabled by NATO's Digital Transformation, to drive military and technological advantages and strengthen the Alliance's ability to operate decisively across various domains [18].

NATO's approach is not isolated but instead relies heavily on cooperation among member nations. Each nation contributes its unique capabilities across various domains, making the collective defense more robust. This fact does not present only opportunities, but also a plethora of challenges:

1. Surprisingly, there is no internationally agreed definition of 'domain' yet, and understandings of what constitutes a domain vary between countries [9, p. 5].
2. Different stakeholders may interpret MDO differently, which can hinder effective implementation. The USA and its allies do not have a consistent way of describing the multi-domain environment. Without this common nomenclature and terminology, it is difficult to have a common understanding of the battlespace.
3. In many cases, the MDO concept does not seamlessly align with existing national political and military structures. The same applies for legal constraints, because planning and execution of MDO across multiple domains, especially cyberspace and the EME, will require an appropriate legal framework, which still needs to be modified or adopted. This fact has become evident during implementation of new capabilities into national armed forces as well as within multinational cooperation of NATO member states.
4. MDO relies heavily on advanced technologies. Ensuring interoperability and reliability across domains remains a challenge.
5. A capability gap is in the capacity of European Allies in U.S. MDO smaller allied states, deploying forces no larger than brigades, to support operations at echelon.
6. Not all allies require the same level of sophisticated equipment to contribute to MDO, but there are three critical challenges to be addressed: shared situational awareness; coordinating synchronic operations at echelon; and the training burden created by the demands of MDO [3, p. 13–14].

To conclude, although NATO has firmly bound the multi-domain approach in its strategic documents, the Alliance is still in the process of fully integrating and operationalizing this approach. To achieve this, clear direction and guidance

from civilian political leaders is essential, along with a common understanding of terms and definitions agreed upon by NATO. This includes developing comprehensive doctrines, capabilities, and training for MDO within the whole Alliance.

4. The Perception of Multi-domain Approach by the Russian Federation and the People's Republic of China

Both the RF and PRC likely view the U.S. MDO concept as a part of broader U.S. strategic intentions, including maintaining global dominance and containing potential adversaries. The concept of MDO is taken up by the Russians as multi-sphere operations (mnogosfernoye operatsii) and by the Chinese as multi or all-domain operations [19, p. 42]. Both countries have already demonstrated a deep understanding of the complexity of MDO by developing their own counter-strategies involving asymmetric warfare, advanced technology investment, and increased focus on information warfare and A2/AD systems (although A2/AD in the Russian context should be rather interpreted as a set of active defensive measures, comprising also offensive capabilities and manoeuvre defence) [20, p. 17].

The RF perceives the U.S. MDO concept as a threat to its national security and strategic interests. Moscow views the concept as an attempt by the United States to maintain its global dominance and to contain Russia's influence. The RF vigilantly observe support of NATO countries to Ukraine, with a special emphasis focused on implementation of new operational concepts. According to Russian sources, the USA exploits the Ukrainian battlespace for testing its MDO strategy, for example by "supporting suppressive and destructive actions against reconnaissance, strike, anti-aircraft, and other combat systems that are carried out simultaneously in several spheres to create numerous difficult-to-resolve problems for the opposing side, which allows identifying vulnerabilities in defense and effectively using the changing situation" [21, p. 126].

The RF has been focusing on developing its own capabilities across multiple domains and geographical regions, including the Baltic, Black and Mediterranean Sea as well as the Artic [18]. A particular emphasis is placed on the whole-of-government approach, ability to repel aerospace aggression with all the strike and defensive capabilities, asymmetric and hybrid warfare tactics, comprising information warfare, radio-electronic combat (i.e. the Russian concept of the electromagnetic warfare), interference in democratic processes, political and economic coercion, malicious cyber activities, and illegal and disruptive activities of Russian intelligence services etc.

To summarize, the RF is using a multi-domain approach to asymmetric warfare against a perceived Western aggressor. This approach focuses on using information to control adversary behavior and shape the strategic environment in Russia's favor. The information environment is seen as the foundation and integrator of all other operational domains, and is therefore critical for achieving asymmetric advantage and Russian success at all levels [9, p. 13].

The PRC acknowledges the existence of the multi-domain approach and most likely has a very accurate understanding of the JADO concept [22]. According to Air Chief Marshal The Lord Stuart Peach *"the PRC has been closely observing the development of the conflict, interprets it in its own way and considers those findings in its strategy"*. [23] It tends to view U.S. military developments through the lens of strategic competition. As such, it is presumed that it sees the MDO and JADO concepts as a potential threat, particularly in the context of the US's focus on the Indo-Pacific region.

The People's Liberation Army (PLA) conceptualizes future warfare as a multidimensional confrontation between competing 'system of systems' which represents a strategic approach that views warfare not simply as a conflict between individual units or platforms, but as a clash between holistic, networked "systems" of weapons, communications, command and control, intelligence, and other military capabilities [9, p. 81]. This approach also emphasizes the integration of different domains of warfare – land, sea, air, space, and cyberspace – into a unified whole, and the use of advanced technology, including artificial intelligence, big data, and automation, to achieve dominance in these domains.

Another PLA concept is represented by 'informationized' warfare which refers to the use of information and communication technologies in modern warfare. It is based on the understanding that information superiority is key to overall military success in contemporary conflicts. In the context of informationized warfare, the side that can gather, process, and use information more effectively will have significant advantages in terms of command and control, intelligence gathering, and the coordination and effectiveness of its forces [24, p. 16].

Therefore, the PRC focus on 'system-of-systems' operations and 'informationized' warfare could be seen as a response to the US's MDO concept, as they share many of the central characteristics of what the West might describe as multi-domain concepts.

5. The Case Study of the Multi-Domain Implication in the conflict in Ukraine

Since the onset of the Russia-Ukraine conflict in 2014, several multi-domain approaches employed by the Russian Federation Armed Forces have been observed. In general, the RF has been utilizing multi-domain concepts to pursue asymmetric 'new-type' and systems warfare, using tactics like 'reflexive control' and disorganisation. The strategy is centered around controlling adversary behavior and shaping the strategic environment in the RF's favor via information use, while also exploiting the adversary's weaknesses to maximize impact with minimal use of the RF's resources. The information environment, which encompasses technological and psychological aspects, have been viewed as a critical foundation that integrates all other operational domains and is thus crucial for the RF to gain an asymmetric advantage and achieve success at all levels of conflict [9, p. 45–65].

This was evident in the Battle of Zelenopillya (2014), where a single Russian Battalion Tactical Group (BTG) commander utilized an array of weapons across multiple domains against Ukrainian forces. The operation stood out due to the strategic integration of organic unmanned aerial vehicles (UAVs), cyber capabilities, and ground forces under the

command of a single battalion, resulting in a synergistic effect. The Russian forces initially launched cyber-attacks to disrupt Ukrainian communications and create confusion in decision-making processes. With the Ukrainian C2 system compromised, the Orlan 10 UAV carried out a meticulous target acquisition of the Ukrainian position, which was subsequently followed by a destructive long-range rocket and artillery strike on the Ukrainian unit. This strategy was replicated in subsequent battles involving different BTGs, including the Battle of Ilovaisk (2014), the Battle of Donetsk Airport (2014–2015), and the Battle of Debal'tseve (2015). The incorporation of Surface-to-Air Missiles (SAMs) and UAVs into the BTG underscores the identified synergies between land and air domains. Additionally, the ground-based jammers' EW capabilities, coupled with EW capabilities embedded in UAVs, demonstrated interconnections between the land and electromagnetic spectrum, as well as with the air domain. These confrontations showed that the strategic use of the cyber domain can create early opportunities for success and facilitate simultaneous offensive and defensive operations across strategic, operational levels, and other domains.

On the other hand, also Ukraine has been employing a multidomain approach in the ongoing conflict with the RF to effectively counteract and respond to the multifaceted threats it faces. With the aid of Elon Musk's Starlink satellite internet service, Ukraine has been able to sustain internet connectivity, demonstrating the application of space domain resources. This comprehensive, multidomain approach has been critical in Ukraine's efforts to resist and respond to the multi-pronged offensive. Elon Musk's involvement in the Russia-Ukraine conflict can be analyzed through the concepts of MDO and MDI. Musk's SpaceX company, through its Starlink satellite internet service, has been providing internet connectivity to Ukraine, an example of operations in the space and cyberspace domains [25]. This has allowed Ukraine to maintain vital communications infrastructure despite Russian attacks, enabling both military and civilian coordination and information dissemination.

In terms of MDO, this can be seen as an example of exploiting the space and cyberspace domains to achieve strategic objectives - in this case, maintaining Ukraine's ability to communicate and coordinate despite adversarial actions. It demonstrates how operations in one domain (space) can affect outcomes in another (cyberspace), and how these can impact the terrestrial battlefield.

Looking at it from an MDI perspective, Musk's involvement illustrates how actions in the space and cyberspace domains can be integrated with operations in other domains. The provision of satellite internet connectivity is not a standalone operation but is integrated with Ukraine's broader military and strategic operations, potentially enhancing their effectiveness.

However, it is crucial to note that while this example fits into the concepts of MDO, it is an unconventional application given that Musk is a private individual and SpaceX a private company, not a state military force. Private companies like SpaceX and Starlink are providing capabilities in the space domain that can be leveraged in multidomain operations. As seen in the recent conflict in Ukraine, where Starlink provided satellite internet service, these capabilities can have a direct impact on the terrestrial domain by enabling communication and information sharing in the face of infrastructure disruption.

In the cyberspace domain, private tech companies play a crucial role in providing cybersecurity solutions and services, which can be integral to the success of multi-domain interrelation. These companies can help protect critical infrastructure, secure communication networks, and respond to cyber threats, which are increasingly being used as a form of warfare. Furthermore, the private sector can also contribute to the development and deployment of emerging technologies like artificial intelligence, machine learning, and unmanned systems, which are likely to play a significant role in future multidomain operations. It is worth to mention that commercial satellite capabilities have increased dramatically, offering eyes in the sky for anyone who wants them. Satellite launches more than doubled between 2016 and 2018; now, more than 5,000 satellites circle the earth, some no larger than a loaf of bread. Commercial satellites have less sophisticated sensing capabilities than do their spying counterparts, but civilian technologies are rapidly improving [26, p. 58].

The significance of nonmilitary means has been underlined also in Russian strategic literature, suggesting that gaining "information superiority" is crucial in accomplishing strategic objectives, including military and other aims. A 2013 article, extensively examined, penned by General Valery Gerasimov, the Chief of the General Staff of the Armed Forces of the Russian Federation, proposed that nonmilitary approaches should play a much more substantial role than military strategies in settling interstate conflicts, suggesting a 4:1 ratio. Identifying and leveraging the weaknesses in the information gaps of opponents are deemed critical to realizing desired political and strategic objectives, especially in an asymmetric competition with adversaries possessing greater military strength [27].

In the past, technological breakthroughs such as the Internet and GPS were pioneered by U.S. government agencies and later commercialized by the private sector. Most innovations that impacted national security didn't have extensive commercial applications, so they could be classified from inception and, if necessary, restricted indefinitely. Today, the situation has reversed. Technological innovations are more likely to be "dual use," having both commercial and military applications. They are also much more likely to originate in the private sector, where they are financed by foreign investors, developed by a multinational workforce, and marketed to global customers in both private and public sectors [26, p. 60].

However, the involvement of private entities in multidomain approach also raises a host of legal, ethical, and security issues. These include questions about accountability, the appropriateness of delegating certain military functions to the private sector, and the need to protect sensitive information and technologies. Therefore, as the role of private entities in MDO continues to grow, it will be important to carefully consider these issues and develop appropriate policies and regulations. This raises interesting questions about the role of private entities in multidomain operations and integration, which could be a fertile area for further research and discussion.

6. The challenges presented by the multi-domain operating environment to Intelligence and ISR

Intelligence naturally spans multiple domains, including the joint, interagency, intergovernmental, and international levels. It plays a crucial role in enhancing lethality by offering efficient and adaptable intelligence backup to large-scale combat operations. Nevertheless, in all strategic military contexts, the importance of intelligence support is paramount. The goal of intelligence is to supply commanders and staff with immediate, pertinent, precise, predictive, and customized intelligence. This information is necessary to understand the OE, evaluate the situation, prepare the theater, guide military actions, and secure relative advantage points across the domains and dimensions of the OE as part of the joint force [6].

One aim of MDO is to disrupt adversary decision-making processes and create multiple dilemmas, which also has implications for intelligence and ISR. The MDO concept requires a high level of interoperability, real-time intelligence sharing, and seamless communication among different military units and platforms. As a result, it heavily relies on advanced technologies such as artificial intelligence, machine learning, and big data analytics. In this respect, it is crucial to note that the successful implementation of the MDO concept depends on the ability to effectively integrate and leverage these technologies. The strategic use of artificial intelligence and machine learning can enable rapid processing and analysis of vast amounts of data, leading to improved decision-making and response times. Moreover, big data analytics can provide valuable insights and predictions, enhancing the situational awareness and strategic foresight of military units. However, the potential challenges such as cybersecurity threats, data privacy issues, and technical complexities should not be overlooked. Therefore, while MDO presents a transformative approach to military operations, it also necessitates concerted efforts in technology integration, cybersecurity measures, and policy development.

Understanding the potential benefits and risks of these and other emerging technologies is a crucial task for intelligence community. Intelligence experts need to identify the frontrunners in pivotal technological races and forecast the possible implications. They must analyze how future conflicts will be conducted and won. It must be ascertained how new technologies could address global issues such as climate change. Intelligence staffs need to discern how adversaries will utilize data and technological tools for coercion, atrocity commission, sanction evasion, dangerous weapons development, and securing other advantages [26, p. 60].

The success of MDO also depends on the ability of military personnel to adapt to the new operational environment, where timely information sharing and collaboration are crucial. Because particular adversary operations within multidomain environment can happen so quickly subject matter experts dealing with the current intelligence also need to operate with newfound speed. For instance, on September 1, 2001, U.S. President George W. Bush had less than 13 hours after the World Trade Center attacks to review intelligence and announce a response. Today, the time for presidents to consider intelligence before making major policy decisions may be closer to 13 minutes or even 13 seconds [26, p. 60]. Therefore, training programs and exercises should be designed to enhance the skills and knowledge of military personnel in the areas of network-centric warfare, decision-making, and mission planning.

To better understand the challenges that the multi-domain operating environment presents to Intelligence and ISR, the authors have examined the respective steps of the UK intelligence process (see Figure 1). Military units and organizations use the intelligence process to integrate intelligence support and provide the commander and staff the intelligence needed to facilitate situational understanding, effectively make decisions, and exercise command and control. The intelligence process consists of four steps (direction, collection, processing, dissemination) [14, p. 38]. Each of these steps is influenced by the multi-domain approach in varying ways and degrees. Findings derived from interviews with intelligence specialists suggest that the MDO have the most significant impact on the second step, "Collection", closely followed by the third step, "Processing". The intensity of the blue color on Fig. 1 visualizes the estimated extent of the "multi-domain impact" on the corresponding step within the intelligence process.

When considering the respective steps of the aforementioned intelligence process, the implementation of MDO presents several opportunities and challenges. One of the key advantages of MDO is the capacity for unified planning and direction, where intelligence requirements from disparate domains are integrated to create a comprehensive intelligence collection plan. This consolidation provides a more holistic operational perspective, enhancing strategic decision-making. Furthermore, MDO broadens the scope of data collection, utilizing resources across multiple domains. This diversification not only increases the volume of information gathered but also enhances the quality and relevance of the intelligence. The processing of this data is expedited by leveraging advanced technologies such as artificial intelligence and machine learning, which are central to MDO. In terms of analysis and production, the integration of data from various domains can lead to a more comprehensive intelligence picture, providing a deeper understanding of the operational environment. This ensures that the intelligence produced is both detailed and accurate. Finally, MDO promotes real-time intelligence sharing and seamless communication among different military units and platforms, which significantly improves the speed and efficiency of decision-making processes.

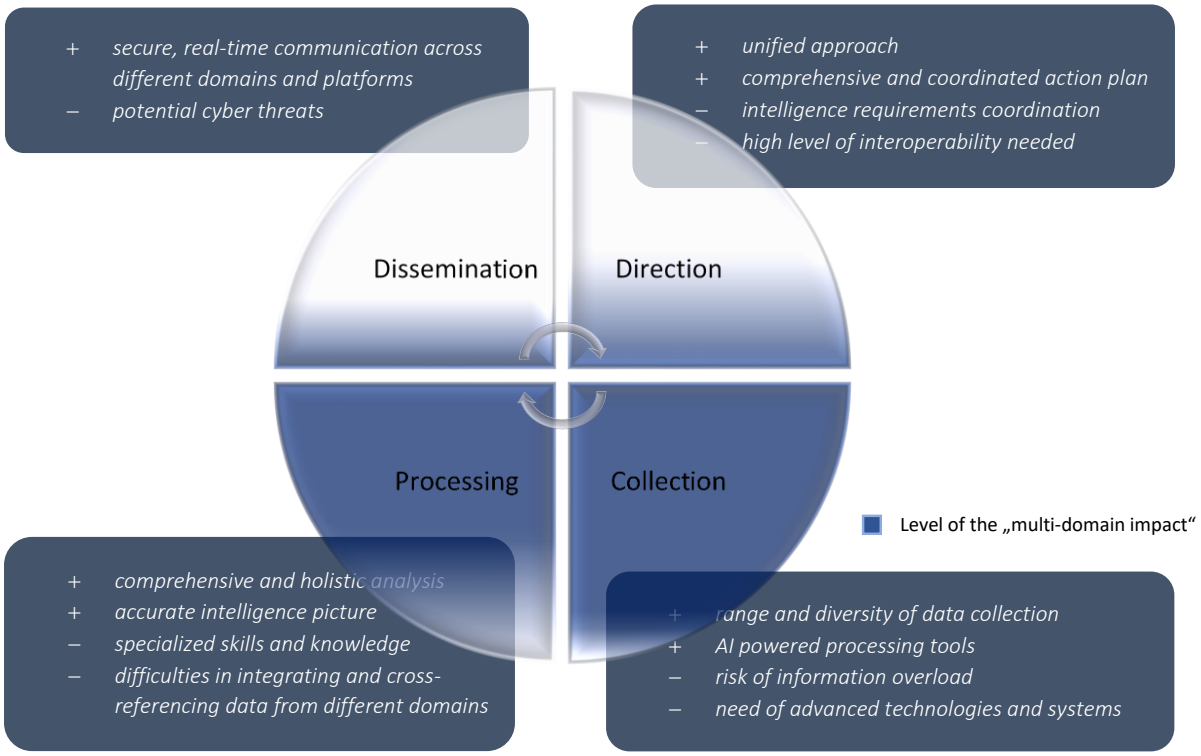

Fig.1. Opportunities (+) and challenges (-) associated with MDO within the intelligence process

However, there are also inherent challenges associated with MDO within the intelligence process. Coordinating intelligence requirements across multiple domains requires a high level of interoperability and coordination, which can be complex. The collection of data from diverse domains can also result in information overload, potentially obscuring relevant intelligence. Processing vast amounts of data from multiple domains necessitates advanced, often expensive technologies and systems, and the analysis of this data requires specialized skills and knowledge. Moreover, ensuring secure, real-time communication across different domains and platforms can be challenging, particularly in the face of potential cyber threats. Thus, robust cybersecurity measures are essential to protect sensitive information. Despite these challenges, the incorporation of MDO into the intelligence process presents a promising avenue for enhancing military operations.

Multi-domain environment is logically affecting also Joint Intelligence Preparation of the Operating Environment (JIPOE) as one of the primary tool used to support joint operation planning, execution and assessment. In this respect, it is not possible to limit the analysis of the contemporary OE only to the physical domains and their relationship to the non-physical ones. Drawing from the authors' extensive experience in NATO multinational intelligence staffs and various intelligence positions across all C2 levels, they contend that the conventional depiction of the OE is inadequate. This depiction, which is heavily reliant on the PMESII-PT model and centers mainly on the physical domains and their connections with the non-physical ones, only offers a narrow understanding of the OE. This is because it does not adequately analyze the synergies and interdependencies that exist between these domains. This applies especially to planning and execution of operations in the non-physical domains, such as electromagnetic operations (EMO), information operations (INFOOPS) or cyberspace operations, where the thorough insight must be obtained in order to identify windows of opportunity in the multi-domain OE, execute faster decision cycles and create synergic effect exploiting collective capabilities available across all the domains.

It is assessed that the current way, in which JIPOE is conducted, provides a solid foundation but it needs to be improved to better accomplish requirements and effectively support of future operations. In order to make JIPOE more relevant and adequate for future military operations, it will be necessary to consider all of the physical and non-physical domains, including the EME, as a combination of tools for achievement of future operational objectives. In other words, it will be very difficult to update and adjust JIPOE processes, if JIPOE primary customers (plans, operations) do not change their pertaining overall perception of the OE. All these aspects will also have to be reflected and described in new or updated doctrinal documents. The application of complex systems through JIPOE can be improved by changing from a categorical description to the interdependency-focused approach, because categories provide descriptions, but interdependencies provides insights [28]. One of the methods, which will have to be introduced and included into JIPOE procedures, is comprehensive risk assessment measuring the impact of threats on multiple assets of the OE. In this way, it will be possible to prioritize the threats, understand interdependencies across the OE or identify centres of gravity more precisely. This intelligence will need to be available in a way that is contextualised to the user. It will also have to be integrated across the C2 to be able to realise windows of opportunity at all levels, thus exploiting the specific conditions and circumstances in the OE.

Despite indisputable benefits of modern technologies, personnel will remain the most critical asset ensuring the cognitive superiority needed for success in future military operations. As of now, education of military professionals in most NATO countries, including members of intelligence staffs, is still focused on tactical level competencies, whereas operational

level knowledge is usually gained during their further military career. Such an approach then creates a widening capability gap, because appropriately qualified military personnel is not always readily available. In order to outcompete opponents in future military conflicts, NATO countries should also update their military education programmes and prepare their personnel how to employ joint capabilities across a multi-domain environment. Hence, in addition to the implementation of cutting-edge technologies as well as conceptual and procedural changes, innovative steps must be taken in relation to the development of expertise and knowledge not only of dedicated OE analysts, but also of all potential customers who are expected to request and use intelligence products in support of future military operations.

7. Conclusions

Multi-domain approach to modern warfare is a holistic one, recognizing the interconnected nature of conflicts and the need for integrated, flexible, and adaptive responses to emerging threats. In this respect, intelligence and ISR staffs will be required to counter numerous challenges ensuing from the dynamic character of the OE and the rapid development of technologies. The authors conclude that despite advances in technology, human factors remain crucial in intelligence operations. This includes the recruitment, training, and retention of skilled intelligence analysts, as well as ensuring effective collaboration and communication among intelligence personnel and with operational commanders.

The analysis reveals that peer adversaries are not merely passive recipients of MDO but active participants who shape and redefine the operational environment. They reflect MDO in their strategic thinking, force structuring, and capability development, indicating a profound understanding of modern warfare's demands. The reflections of MDO by peer adversaries underscore the evolving character of modern warfare. Recognizing these reflections is essential for adjusting defense strategies and understanding the changing dynamics of international security. Future research should focus on exploring specific cases of peer adversaries' reflections on MDO to provide more nuanced insights.

The role of intelligence and ISR will be of the paramount importance, because commanders must be provided with timely information they need to make informed decisions and effectively employ forces across various domains., including information overload, cross-domain integration of data and intelligence obtained from multiple domains, or complex synchronization of ISR assets in the diverse and contested OE [29, p. 114]. This will not be possible without implementation of new technologies, such as artificial intelligence and big data processing to enable effective intelligence processing and analysis.

References

1. U.S. ARMY, 2022. *FM 3.0 Operations*. Online. Washington: Headquarters Department of the Army. Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf.
2. *Sun Tzu - Quates*, 2024. Online. In: Good Reads. Available at: https://www.goodreads.com/quotes/233643-there-are-not-more-than-five-musical-notes-yet-the.
3. WATLING, Jack and ROPER, Daniel, 2019. *European Allies in US Multi-Domain Operations*. Online. RUSI. Available at: https://www.rusi.org/explore-our-research/p publications/occasional-papers/european-allies-us-multi-domain-operations.
4. *The U. S. Army in Multi-Domain Operations 2028*, 2018. Online. TRADOC. Available at: https://www.tradoc.army.mil/wp-content/uploads/2020/10/TP525-3-1-The-Army-Operating-Concept.pdf.
5. FEICKERT, Andrew, 2024. *Defense Primer: Army Multi-Domain Operations (MDO)*. Online. 2nd. Washington, D.C.: Congressional Research Service. Available at: https://crsreports.congress.gov/product/pdf/IF/IF11409.
6. U.S. ARMY, 2022. *FM 2.0 Intelligence*. Online. Washington: Headquarters Department of the Army. Available at: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN39259-FM_2-0-000-WEB-2.pdf.
7. BRONK, Justin and CRANNY-EVANS, Samuel, 2022. Building the Capacity to Conduct Joint All-Domain Operations (JADO): Considerations for the UK. Online. RUSI. Available at: https://rusi.org/explore-our-research/publications/occasional-papers/building-capacity-conduct-joint-all-domain-operations-jado.
8. TAYLOR, Nuray, 3 Nov 2021. What is JADO? Online. In: Signal–Media. Available at: https://www.afcea.org/signal-media/what-jado.
9. BLACK, James; LYNCH, Alice; GUSTAFSON, Kristian; BLAGDEN, David; PAILLE, Pauline et al., 2022. Multi-Domain Integration in Defence. Online. RAND Corporation. Available at: https://www.rand.org/pubs/research_reports/RRA528-1.html.
10. Summary of the Joint All-Domain Command and Control (JADC2), 2022. Online. Department of Defense. Available at: https://media.defense.gov/2022/mar/17/2002958406/-1/-1/1/summary-of-the-joint-all-domain-command-and-control-strategy.pdf.
11. Battle Management. DOD and Air Force Continue to Define Joint Command and Control Efforts., 2023. Online. Washington, D.C.: United States Government Accountability Office. Available at: https://www.gao.gov/assets/gao-23-105495.pdf.
12. KIELEY, Marc, 2021. EXQUISITE CAPABILITIES VS STRATEGIC INTEGRATION: US AND UK APPROACHES TO MULTI-DOMAIN OPERATIONS AND IMPLICATIONS FOR THE CANADIAN ARMY. Online, Service Paper. Canadian Forces College. Available at: https://www.cfc.forces.gc.ca/259/290/23/192/Kieley.pdf.

13. Joint Concept Note 1/20. Multi-Domain Integration, 2020. Online. London: Ministry of Defence. Available at: https://assets.publishing.service.gov.uk/media/6579c11a254aaa000d050c6e/20201112-ARCHIVE_JCN_1_20_MDI_Official.pdf.
14. Joint Doctrine Publication 2-00. Intelligence, Counter-intelligence and Security Support to Joint Operations., 2023. Online. 4th. London: Ministry of Defence. Available at: https://assets.publishing.service.gov.uk/media/653a4b0780884d0013f71bb0/JDP_2_00_Ed_4_web.pdf.
15. Brussels Summit Communiqué: Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021, 14 Jun 2021. Online. In: North Atlantic Treaty Organisation. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm?selectedLocale=en.
16. NATO 2022 Strategic Concept, 2022. Online. Brussels: NATO. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.
17. JOHNSON, David, 14 Jun 2022. The Army Risks Reasoning Backwards in Analyzing Ukraine. Online. In: War on the Rocks. Available at: https://warontherocks.com/2022/06/the-army-risks-reasoning-backwards-in-analyzing-ukraine/.
18. Vilnius Summit Communiqué: Issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Vilnius 11 July 2023, 11 Jul 2023AD. Online. In: North Atlantic Treaty Organisation. Available at: https://www.nato.int/cps/en/natohq/official_texts_217320.htm.
19. TOURETT, Vincent, 2021. Russian and Chinese multi-domain approaches: the same aerospace battle? Online. In: Institut de Recherche Stratégique de l'Ecole Militaire. Available at: https://www.irsem.fr/media/documents-en-anglais/4-russian-and-chinese-multi-domain-approaches.pdf.
20. KOFMAN, Michael; FINK, Anya; GORENBURG, Dmitry; CHESNUT, Mary; EDMONDS, Jeffrey et al., 2021. Russian Military Strategy: Core Tenets and Operational Concepts. Online. The Center for Naval Analyses. Available at: https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts.
21. VODZYANSKIY, S. I., 2023. Multi-Domain Battle as a Result of the Evolution of Joint Actions by Various Types of U.S. Military Forces in the 20th-21st Centuries. Online. Voennaia Mysl. 105, No. 8, p. 125–133. Available at: https://vm.ric.mil.ru/upload/site178/zLvI4uxWeg.pdf.
22. SOLEN, Derek, 2020. Chinese Views of All-Domain Operations. Online. In: The Department of the Air Force's China Aerospace Studies Institute. Available at: https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/CASI%20Articles/2020-06-30%20Chinese%20Views%20of%20All-Domain%20Operations.pdf?ver=0gVa73tTs6oxBmMIQnTYxg%3D%3D.
23. PEACH, Stuart. Conference Keynote Address. AOC Europe Conference. 14 May 2024. Oslo, Association of Old Crows.
24. MCINNIS, J. Matthew, 2023. Russia and China Look at the Future of War. Online. Washington, D.C.: Institute for the Study of War. Available at: https://www.understandingwar.org/sites/default/files/Russia%20and%20China%20Look%20at%20the%20Future%20of%20War_0.pdf.
25. What has Elon Musk said about Russia's war in Ukraine?', The Independent. Accessed: Mar. 06, 2024. [Online]. Available: https://www.independent.co.uk/news/world/europe/elon-musk-ukraine-starlink-b2282465.html
26. ZEGART, Amy. "Open Secrets." Foreign Affairs, Dec. 20, 2022. Available at: https://www.foreignaffairs.com/world/open-secrets-ukraine-intelligence-revolution-amy-zegart
27. KERR, Jacklyn, 2023. Assessing Russian Cyber and Information Warfare in Ukraine: Expectations, Realities, and Lessons. Online. Washington, D.C.: The Center for Naval Analyses. Available at: https://www.cna.org/reports/2023/11/assessing-russian-cyber-and-information-warfare-in-ukraine.
28. PIKE, Thomas, 2020. Analysis and Artificial Intelligence in Integrated Campaigning 2019. Online. NSI. Available at: https://nsiteam.com/analysis-and-artificial-intelligence-in-integrated-campaigning/.
29. ŽÁRSKÝ, Petr, Petr HLAVIZNA a Jakub HNIDKA. Využitelnost multikoptér v Armádě České republiky. Vojenské rozhledy. 2022, 31 (2), 106-120. ISSN 1210-3292 (print), 2336-2995 (on-line). Available at: www.vojenskerozhledy.cz.