UNDERSTANDING MULTI-DOMAIN OPERATIONS FROM THE AIR FORCE PERSPECTIVE

George–Adrian AIONESEI[*], Cristian PANAIT[**]

[*]Boboc Air Force Base, Buzău, Romania (aioneseiadrian11@gmail.com),
[**]"Henri Coandă" Air Force Academy, Braşov, Romania (cripanait@gmail.com)

DOI: 10.19062/1842-9238.2024.22.1.8

Abstract: *This document delves into the transformative shift in military strategy towards Multi-Domain Operations, dictated by the fast evolution of warfare technologies and the complex nature of the contemporary battlefields. It outlines the historical progression of warfare from domain-specific tactics to the integrated approach of MDOs, emphasizing the importance of synchronizing operations across land, air, sea, space and cyberspace to achieve operational superiority. The air force's critical role in this paradigm is highlighted, including its capabilities in air and space superiority, intelligence, surveillance, reconnaissance, rapid global mobility, and command and control. There are also discussed the challenges such as interoperability, technological adaptation and training for MDOs, as well as the future success of military operations which fosters collaboration and innovating training programs to effectively counter adversaries in this new era of warfare.*

Keywords: *multi-domain, air force, warfare, operations.*

1. INTRODUCTION

One of the main reasons to change the way military forces conduct their operations, either offensive or defensive, is based on the changes that take place at the technology and maneuver levels. When a new technology is involved in the battlefield, the tactics, techniques, procedures and ultimately the doctrines have to be changed accordingly in order to have the advantage over the enemy.

Looking back, hand-to-hand combat was a defining feature of early warfare, with methods and tactics frequently constrained by weapon technology and soldier physical prowess. As civilization advanced, so did the military technology and organizational systems, leading to evolution of specialized units such as cavalry and archers.[1] Then, the introduction of gunpowder in the warfare, and the rise of artillery and infantry equipped with firearms transformed the way of battles, sending the troops into the trenches [2]. This became the time of modern armies as permanent and professional establishments and the development of navy and maritime battles.[3] The next important episode in the warfare evolution consists of the Industrial Revolution, which brought important advancements in weaponry and logistics, enabling mass production of arms and the use of large-scale forces into the battlefield. The power of modern industrialized warfare was demonstrated in World War I and World War II with new technologies such as tanks and aircrafts, innovations that rapidly changed the nature of conflict.[1] The Cold War and the Nuclear Age, another shift in the warfare, focused on the nuclear arms race and a strategy of deterrence between big states. As a result, based on the threat of mutual destruction, the international relations were reshaped. The conventional forces were not

eliminated, but the attention was shifted more towards strategies of potential global annihilation.[4] The last important stage of technology advancement lays in the information age and the network-centric warfare in the late 20th century, which reduces the classic physical warfare and emphasizes the power of information in order to boost situational awareness, speed of reaction and command, and the ability to be more precise and efficient. The development of the satellite communications and surveillance made it possible for space-based capabilities to be integrated within traditional military operations.[5]

Each historical phase demonstrates an incremental move towards the principles that laid the foundation for how the military operations are conducted today. The shift from separated domain-specific tactics to integrated multi-domain strategies shows the continuous adaptation of military thought to take advantage of communication and technological breakthroughs, reflecting the complexity of contemporary international warfare.

2. MULTI-DOMAIN OPERATIONS

Having in mind how the technology has changed the history through some important milestones, those milestones in their turn, had their contribution to the ways in how the wars were organized and conducted from the strategic point of view. At first, the land and sea domains were seen as the main means through which the military, political and economic powers were projected in the battlefield. The fast advancements in aviation led the air domain to become equal as importance to land and maritime domains in operations such as The Blitz (1940-1941), The Berlin Airlift (1949) or Operation Desert Shield and Desert Storm (1991). Many military campaigns, since World War I, have been carried successfully with an effective and powerful collaboration between the three domains [6].

With the base of the pyramid formed, it was only a matter of time until a new domain will take place in the warfare spectrum: the space power. Gulf War (1990-1991), the invasion of Afghanistan in 2001 and the invasion of Iraq in 2003 were some occasions where all four fields were put together, with the space having a special contribution [7]. The last domain that closed the circle was cyberspace, a domain that was firstly used with 2010 Stuxnet, the first genuine cyberweapon designed to inflict physical damage, which ruined almost 20% of Iran's nuclear centrifuges [8]. Even though space and cyberspace present a few limitations regarding geography, these five domains that drew their attention through time, complete the operational environment for which military experts and leaders must prepare in the current century. This environment refers to the new concept introduced by the United States of America Army in 2018, as Multi-Domain Operations (MDO). The future conflicts will not be restricted to single domains (land, sea, air), but will encompass other areas such as space, cyberspace or electromagnetic spectrum. It reflects an understanding of the complex and interconnected battlefield of the current century, where military warfare goes asymmetrical with the possibility of battles in multiple arenas.[1]

The full definition of the term Multi-Domain Operations (MDOs) has not reached its final stage, as many states or entities have different ways of defining it. The terms "multi" (multiple) or "operations" do not represent a matter as to what they signify, but the issue becomes more complex when military professionals try to agree on the meaning of the term "domain". This term has multiple connotations outside of the military environment; therefore, the military is in the position of not only clarifying the meaning of the word itself, but to ensure the definition is different from the usage outside the military context.

A definition proposal that was accepted by many is the one the director of Multi-Domain Operations Strategists concentration of the US Air Forces Air Command and Staff College, Jeffrey Reilly gave, such as a "domain is a critical macro maneuver space whose access or control is vital to the freedom of action and superiority required by the mission" [9]. Simply put, a domain represents an accessible area, which is not necessary to be physical, where there can exist modifications.

The definition of MDOs is an issue highlighted by the differing terminologies and concepts used within and among NATO allies. The U.S. Department of Defense (DOD) officially adopts the term JADO (Joint All Domain Operations) [10], while the U.S. Army refers to it as MDO. Canada prefers the term pan-domain operations [11] whereas other NATO members and NATO itself generally use MDO. In The US Joint Publication 3-0 (JP 3-0), MDO takes the form of Operational Environment which encompasses physical areas of land, maritime air, space and cyberspace as well as the electromagnetic spectrum and involve conventional, special operations, ballistic missile, electronic warfare and information capabilities [12]. In the US Army Multi Domain Operations 2028 document, the term MDOs is defined as "operations conducted across multiple domains and contested spaces to overcome an adversary's strengths by presenting them with several operational and/or tactical dilemmas through the combined application of calibrated force posture" [13]. For the Nord Atlantic Treaty Organization (NATO), as its core, MDO refers to the push for the organization to orchestrate military activities across all operating domains and environments. These actions are synchronized with non-military activities and enable the Alliance to create desired outcomes at the right time and place [14]. It effectively frameworks the leaders of NATO vision towards military and political levels for an adaptable, MDO-enabled alliance capable to outsmart and outpace the enemies.

The crucial first step requires a careful understanding of the elements of the operational environment and the relations between them, which makes possible the cross-domain synergy.[15] As stated in the JP 3-0, an operational environment consists of two big elements, the five physical domains: land, maritime, air, space, cyberspace (which transits the other four domains through nodes encompassing both civilian and military entities) and the three dimensions: physical, information, human, which can be analyzed at the level of each individual domain [12]. If commanders and staff are able to understand the physical, information and human dimensions corresponding to all domains, they have the advantage to asses and anticipate the impacts of their operations. A representation of these domains and dimensions is illustrated in Fig. 1.

Understanding each domain and dimension is crucial for developing comprehensive military strategies that leverage the full spectrum of capabilities in contemporary conflict environments.

Domains in MDOs:

- **Land** – this domain is the traditional sphere of military operations, involving securing territory, controlling population centers and engaging with enemy ground forces. Its complexity has increased with the advent of urban warfare and asymmetric threats, requiring a continuous adaptation;

- **Maritime** – this domain includes the world's oceans, seas and waterways, and the maritime operations focus on securing sea lines of communications, projecting power ashore and denying adversaries the use of maritime routes. It is essential for the movement of military forces and equipment;

- **Air** – it encompasses the airspace above the land and sea, including aircraft, satellites and associated infrastructure, and enables the projection of power, rapid mobility of forces, intelligence, surveillance and reconnaissance capabilities and direct support to ground and sea forces;

- **Space** – it includes the area above the Earth's atmosphere where satellites operate and provides critical capabilities such as communication, navigation, early warning systems and intelligence, surveillance and reconnaissance (ISR);

- **Cyberspace** – this domain has the global network of information technology infrastructures, including Internet, telecommunications network, computer systems. The operations in cyberspace can influence the outcome of conflicts in other domains by disrupting enemy communications, gathering intelligence, and manipulating information.

Dimensions in MDOs:

- **Physical** – this dimension refers to the tangible aspects of military operations, including personnel equipment, infrastructure, and the geographic environment. This dimension is closely associated with traditional concepts of warfare but is increasingly integrated with actions in the information and human dimensions;

- **Information** – it encompasses the collection, management, protection and dissemination of information. It includes cyber operations, electronic warfare, and psychological operations aimed at influencing, deceiving, or disrupting the enemy's decision-making processes.

- **Human** – it focuses on the influence of operations on human behavior, beliefs, and decision-making. This includes the morale of forces, the support of local populations and the perceptions of the international community.

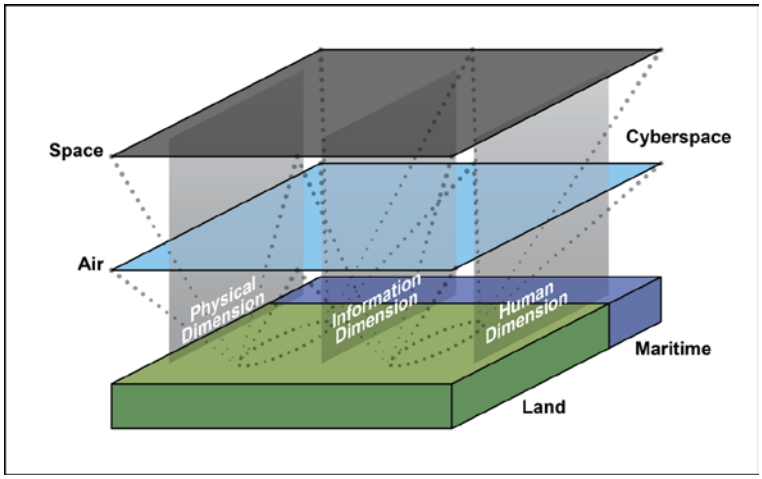

FIG. 1. Domains and dimensions of an operational environment (1) – FM 3-0-000

3. TAKEWAYS FROM THE RUSSIA-UKRAINE WAR

Since February 22nd 2022, when Russia began the invasion of Ukraine, the multitude and continuous military operations constituted an uncertainty of what would happen next. This ambiguous "fog of war" of what is occurring during combat could be considered an important factor [16], and even though the future of war cannot be exactly predicted, this conflict holds a series of lessons for NATO on how to adapt and integrate MDOs.

The conflict has highlighted the pivotal role of the cyber domain in modern warfare, demonstrating that cyber resilience and offensive capabilities are essential components of national defense strategies. Even before the invasion on February 2022, Russia used cyberattacks against Ukraine, focusing on distributed denial-of-service (DDoS) on websites across multiple sectors, including one of the Ukrainian Ministry of Defense on February 15th [17], or sending wiper malware programs to erase data, programs or hard drives, to the main institutions of government, financial, information technology and energy sectors [18]. Also, the Ukrainian Internet services were temporarily affected in

aimed attacks to telecommunication systems [19]. Besides disruption and disruptive attacks, data weaponization (acquisition of data for espionage, surveillance and intelligence purposes) and disinformation were used before and after the invasion [20]. The cyber resilience that Ukraine inflicted against Russian attacks was critical for military, as well as for the economy and civilian part. The key for success laid in the high degree of collaboration between other nations governments and public institutions [21].

One of the main lessons that can be derived from this is that the cyber element, as part of MDOs, is able to connect kinetic and cyber operations. Just before the conventional invasion by Russia on land, the cyberattacks on computers, modems that communicate with satellites, or networks, were a great distraction for Ukrainian forces and for its command and control. A second outdraw consists of the participation of non-traditional actors engaged in cyberattacks [22]. After the attack on satellite communications infrastructure, because the Ukrainian military and government could not use the satellite communications anymore, SpaceX offered free access to their network, Starlink satellite Internet services. The replacement was welcomed and used as primary network, proving to be resilient against signal jamming too [23].

On another level, a main characteristic of the Russia-Ukraine War since the beginning of it has been the utilization of Unmanned Aerial Systems (UAS) on the battlefield. The use and advancement of UAS have highlighted broader trends in drone technology and its integration into high-intensity conflicts of contemporary battlefield. The Unmanned Aerial Vehicles (UAVs) were present since the early stages of the war. Ukraine used the Bayraktar TB2, whilst Russia used Kronshtadt Orion, Korsar and Forpost-R. The use of these types of drones was mainly for ISR, and electromagnetic warfare (EW) as well as precision strikes, but in time, they showed to be expensive and unreliable in enemy's airspace as the air superiority could not be achieved through them [24]. Therefore, both parties searched for alternatives and the solution was to have smaller and more cost-effective UAVs, rather than big and easier to target drones. The drone dynamics in Ukraine have showed class I (less than 150 kg) and class III systems (greater than 600 kg). While large drones equipped with missiles can cause significant destruction in scenarios where air superiority is established, smaller drones were becoming essential for providing ground troops and mobile units with critical situational awareness. Moreover, small and inexpensive "kamikaze" drones offered an alternative method for delivering explosive payloads [25]. Another utilization of drones over the last two years is that both Ukraine and Russia managed to integrate UASs in their command-and-control organizations through the "kill chains" concept – a process of understanding the battlefield, identifying a target, determining the target's location, deliberating what action to take and deciding the best course of action for gaining the advantage [26]. Even though the EW was used and prevented the ISR mission, both parties managed to gather the needed information in order for the military leaders to know the battlefield and to make their decisions accordingly.

The use of UASs in the Russia-Ukraine conflict underscores their strategic and tactical significance across all domains of warfare. Their flexibility, cost-effectiveness and capability to operate in high-risk environments make them indispensable tools in achieving multidimensional operational objectives. While UAVs are being used in the conflict on multiple fronts, they are expected to have a critical role in the future for both Russia and Ukraine. Thus, the battlefield will become the main source of ideas for the development for new and more efficient drones for future conflicts [27]. As the conflict progresses, the evolving use of UAS will likely continue to shape the tactics and strategies employed by both sides, showing the critical role of unmanned systems in contemporary and future warfare scenarios.

The conflict between Russia and Ukraine might be far from over, but besides the negative effects that brings to both countries and also to the entire world, it shows evolution on different domains and ways of how to approach the current and future warfare. NATO as an alliance and all the nations at the individual level are able to learn from this conflict how to integrate critical factors into their defense systems and how to manage a possible confrontation with a belligerent. Also, the takeaways from this conflict and others can help to shape the MDOs to the point it does not raise any concern on its definition or how it can be applied in the warfare.

4. AIR FORCE AND MULTI-DOMAIN OPERATIONS

Besides the Russia-Ukraine war, by looking at the global campaigns there can be analyzed the possibilities of how the components of MDOs can be related and used in order to be central for every operation. For example, if there is a military engagement of NATO with Russia, there will be mainly an air, space and land campaign with the help of the maritime component. If there is a campaign in the Pacific, mainly it will be a maritime, air and space campaign with a small implication of the land element. For a Middle East campaign, there will be the air and space elements first, after which the land and maritime components will enforce the operation. What it can be withdrawn from these examples and from the military events that were conducted in the past, is that the air and space components (once considered as one element) are the ones that need to be present and engaged in most of the military operations either small or regional to global ones.

Air forces, at the global level undertake a diverse range of operations beyond the traditional domain of air combat to strengthen regional stability and address security challenges. The core missions of air forces encompass air and space superiority, ISR, rapid global mobility, global strike, and command and control (C2). Every nation and alliance that possesses an air force, defines its role and tasks clearly in order to create a safe air space for itself and for the allies. NATO Joint Air Power has a key role in accomplishing its three main tasks: collective defense, crisis management and cooperative security, through its three main attributes: speed, reach and height. The alliance is faced with threats and challenges, from either state or non-state actors (Russia, China), terrorism, and cyber-attacks, which are more complex nowadays. As air and space overlay the globe, the organization must be able to employ air power in all possible terrains and environments [28].

For another instance, the Royal Air Force (RAF) is involved in multiple operations across the globe, highlighting the importance of air forces in preserving stability and assisting allies on a global scale. Important RAF activities include the establishment of the UK Space Command to defend space domains, support for the COVID Aviation Task Force in the UK, and Operation SHADER against Daesh in Iraq and Syria. In order to improve coordination and readiness among NATO partner countries, the RAF also takes part in a number of exercises, such as Exercise Point Blank alongside the US Air Force and NATO Air Policing missions in the Eastern side of Europe [29].

In addition to these operations, the Air Force Global Strike Command (AFGSC) highlights the strategic capabilities of the U.S. Air Force, overseeing all long-range nuclear-capable bomber and intercontinental ballistic missile forces. This includes managing bombers like the B-52 Stratofortress, B-1 Lancer, and B-2 Spirit, which are essential for global strike capabilities and deterrence strategies [30].

In MDOs, the air force’s role is pivotal as it moves towards a fully networked, integrated approach to modern warfare, where victory hinges on the cohesive operation of

networks, sensors, and systems across air, space, sea, cyber and information domains. General David L. Goldfein, the 21st US Air Force Chief of Staff, emphasized that the future of combat would depend less on individual platform capabilities and more on the integrated strengths of a connected network. The Air Force aims to create a force where every asset is interconnected, transforming the way information is collected, assessed, and transmitted, thereby producing multiple dilemmas for adversaries to overwhelm them [31]. He also suggested that MDOs would change the character of warfare by utilizing dominance in one or many domains to create overwhelming challenges for adversaries and find their vulnerabilities.

As a general aspect, the main contributions that the air force can bring to its domain in order to create a secure and efficient environment when it comes to MDOs consist in:

- Rapid global mobility and reach;
- Air superiority and space control;
- Intelligence, Surveillance and Reconnaissance (ISR);
- Precision strike capabilities;
- Command and control (C2);
- Adaptability and innovation;

The air force's role in MDOs is multifaceted, usable cross-domains and by leveraging its strengths and integrating with other services and allies, it significantly contributes to the effectiveness and success of MDOs. Until the point where MDO can be utilized at its full potential, integrating in the most efficient ways all domains with all their characteristics, in order to complete an objective flawlessly, military and political experts also need to analyze the barriers that might be encountered along the way and also the future implications that the air forces have to face.

5. CHALLENGES AND FUTURE IMPLICATIONS OF AIR FORCE IN MDOs

MDOs might be considered a shift from traditional joint operations towards operations that leverage capabilities across multiple domains simultaneously, demanding significant adaptations in command and control, connectivity, interoperability, technology and training.

Interoperability and technology play critical roles in enabling MDOs, requiring robust real-time intelligence sharing among allies. The political will to share data is often a bigger barrier than technical connectivity. NATO allies need to work towards a unified multi-domain strategy, involving political decision-makers in the process to ensure necessary intelligence sharing and establishing a legal framework for operations. This interoperability is essential for creating a common operating picture and ensuring the effectiveness of MDOs across allied nations.

Training and personnel development are also crucial for the successful implementation of MDOs. A bottom-up cultural change in the education and training process of military personnel is required to develop an appreciation and understanding of MDOs. The establishment of a formal cadre for dedicated Multi-Domain Command and Control (MDC2) experts and the development of MDO training infrastructures using live, virtual and constructive training paradigms are steps towards achieving this. Once the MDC2 is formed and effectively used, in order to enable it to a larger scale, the nations and the alliance need to take in consideration the connectivity at the information level. A potential combat cloud might be the solution for centralization of all the information that afterwards can be shared to multiple entities. At the same time, all members could generate more data with their own sensors and systems and update the cloud in real-time. Such measures will enhance decision-making in MDOs and simulate complex threat

environments, preparing personnel for the integrated operational demands of future conflicts [32].

The transition to MDOs involves a few implications that are crucial for understanding the new concepts that emphasizes the inherent cooperation and interoperability within air forces, expanding from traditional airpower to integrating kinetic and non-kinetic effects across multiple domains in real-time [13]. In the future, as shown by the German Luftwaffe, MDO needs to find its place into every nation and alliance's mindset in order to create a desirable advantage over others. This involves embracing the importance of cyber and space, which are crucial to all other domains. Cyber actors can change their environment to both their advantage and their enemies' disadvantage, and space actors have direct contact and access to all traditional domains.

To ensure the success of joint all domain operations (JADO), the C2 must give up the traditional way of thinking and leave behind the well-used and rigid hierarchical command structure at all levels. The air dimension might be the perfect one to provide the tactical part of distributed control if the electromagnetic environment (component of the cyber domain) is well managed across all domains. Multi-domain C2 requires dynamic action at the tactical level, with agile decision making critical to the success of joint all domain integration. In the area of information processing, the C2 needs to take a new approach. The air force can generate an immense amount of data, but the main concern lays in what information should be shared and with whom, to best enable the delivery of the right effect at the right place and time.

Another aspect regarding the application of MDOs in the future refers to the selection of the systems that need development for new needs or requirements and systems that do not fully meet the modern technological requirements or are efficiently enough. As an alliance, NATO's air force should focus on unfolding the full potential by integrating besides the newest technology, older weapons (such as 4^{th} generation fighters – Eurofighter, Rafale, Hornet, Gripen) effectively into the multi-domain concept. For this purpose, the best approach is to participate at as many international exercises, an approach that will focus on multinational cooperation, the basis of interoperability [33].

The last implication for the future of MDOs is of a greater importance, because it is located at the core of the concept. The need of a vision through many small steps can be materialized by sharing information, ideas and theories but also by cooperating in early testing and technology development. These will be achievable by a few short and medium-term approaches that will focus on the best resource that every military forces have: the personnel. Moving forward, education, training and leadership will be the key to train the airmen in a multi-domain manner. These will be introduced from the beginning of career and at every step where it is necessary in order to fulfill the long-term vision.

6. CONCLUSION

The evolution of warfare and the beginning of MDOs mark a transformative period in military strategy, where the integration of capabilities across land, air, sea, space and cyberspace domains becomes essential for achieving operational superiority. This comprehensive approach reflects the recognition of the complex, interconnected nature of contemporary battlefields, where traditional domain specific tactics are insufficient. The air force, with its pivotal roles in air and space superiority, rapid global mobility, precision strike capabilities, ISR and command and control, emerges as a central figure in the successful execution of MDOs. Challenges such as interoperability, technology adaptation and the development of a multi-domain mindset underscore the need for enhanced collaboration, innovative training programs, and a forward-thinking approach to harness

the full potential of MDOs. The future of warfare demands a dynamic, agile military force capable of leveraging the synergistic effects of joint domain operations to outmaneuver adversaries. By embracing the principles of MDOs and fostering a culture of continuous learning and adaptation, military forces can maintain strategic advantage and ensure security in an increasingly complex and technologically advanced environment.

The concept of MDOs as a whole and specific to each domain is still in an initial phase. This article aimed to provide a summary of information to lead to a better understanding of the existing bibliography in the field.

REFERENCES

[1] K. Nettis (2020, March 16). *Multi-Domain operations: bridging the gaps for dominance*, 16 March 2020, Air University (AU), Available at www.airuniversity.af.edu, accessed on 11 Mar 2024;
[2] N. Murray, *The Rocky Road to the Great War: The Evolution of Trench Warfare to 1914*, Washington, DC: Potomac Books, 2013;
[3] J. Kelly, *Gunpowder: Alchemy, Bombards, & Pyrotechnics: The History of the Explosive that Changed the World*, Basic Books, 2005, pp. 95-96;
[4] J.L. Gaddis, *The Cold War: A New History*, The Penguin Press, New York, 2005;
[5] J. L. Groh, *Network-Centric Warfare: Leveraging the Power of Information*, U.S. Army War College Guide to National Security Policy and Strategy, 3rd Edition, vol. I, pp. 323-334, 2008;
[6] Gen. W.S. Wallace, *Multi-Domain Operations in Context*, The Landpower Essay Series, The Association of the United States Army, 2020;
[7] Col. M.J. Lyons, U.S. Army and Col. D.E. Johnson, *People Who Know, Know MDO, Understanding Army Multi-Domain Operations as a Way to Make it Better*, The Landwarfare Papers, The Association of The United States Army, 2022;
[8] T. Orr, *A Brief History of Cyberwarfare*. GRA Quantum, 11 November 2018, https://graquantum.com/a-brief-history-of-cyberwarfare, accessed on 09 Mar 2024;
[9] J. Farley, *Reilly Multi-Domain Final*, 10 Apr 2018, Video on YouTube, https://www.youtube.com/watch?v=jcTicq1BagM, accessed on 12 Mar 2024;
[10] Air Force Doctrine Publication 3-99, U.S. Air Force and U.S. Space Force, 2021, pp. 1-4;
[11] Lt.col. P.J.G. Perron, *Pan-Domain Operations: How can the Canadian Army Prepare its Forces and Contribute to Multi-Domain Coalitions?*, Canadian Forces College, 2020;
[12] US Joint Publication 3-0, Joint Operations, 17 Jan. 2017, Incorporating Change 1, 22 Oct. 2018;
[13] TRADOC Pamphlet 525-3-1, United States Army Training and Doctrine Command, *The U.S. Army in Multi-Domain Operations 2028*, Army Training and Doctrine Command, 2018;
[14] *Multi-Domain Operations in NATO – Explained*, NATO ACT, October 5, 2023;
[15] M. Balboni, J. A. Bonin, R. Mundell, D. Orsi, C. Bondra, A. Dunmyer, L. Marks, *The Need for Multi-Domain Operations: In Mission Command of Multi-Domain Operations*, Strategic Studies Institute, US Army War College, 2020, pp. 17–32;
[16] S. G. Jones, J. Harrington, C. K. Reld & M. Strohmeyer, Ukraine War. In *Combined Arms Warfare and Unmanned Aircraft Systems: A New Era of Strategic Competition*, Center for Strategic and International Studies (CSIS), 2022, pp. 16–24;
[17] K. Fendorf and J. Miller, *Tracking Cyber Operations and Actors in the Russia-Ukraine War*, Council on Foreign Affairs, 24 March 2022, https://www.cfr.org/blog/ tracking-cyber-operations-and-actors-Russia-Ukraine-war, accessed on 13 Mar 2024;
[18] Cyber Peace Institute, *Cyber Dimensions of the Armed Conflict in Ukraine, Quarterly Analysis Report Q3 July to September 2023*, 2023;
[19] L. Herbert, *Russian Cyber Operations in the Invasion of Ukraine*, *The Cyber Defense Review*, vol. 7, no. 4, 2022, pp. 31–46;
[20] Microsoft Corporation, *Defending Ukraine: Early lessons from the Cyber War*, 2022, Retrieved March 15, 2024, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK;
[21] M. Willett, *The Cyber Dimension of the Russia–Ukraine War*. Survival: October-November 2022, vol. 64, Issue 5, 2022, pp. 7-26;
[22] S. Duguin and P. Pavlova, *The role of cyber in the Russian war against Ukraine: its impact and the consequences for the future of armed conflict*. European Parliament, 2023, https://doi.org/10.2861/800788;
[23] M. Rothman, L. Peperkamp and S. Rietjens, *Reflections on the Russia-Ukraine war*, Leiden University Press, 2024, pp. 69-70;

[24] F. Borsari and B. Gordon, *An Urgent Matter of Drones: Lessons for NATO from Ukraine—CEPA*, 2023, https://cepa.org/comprehensive-reports/an-urgentmatter-of-drones/, accessed on 16 Mar 2024;
[25] K. Dominika, *The war in Ukraine shows the game-changing effect of drones depends on the game*, Bulletin of the Atomic Scientists, pp. 95-102, 2023, DOI: 10.1080/00963402.2023.2178180
[26] C. Brose, *The Kill Chain: Defending America in the Future of High-Tech Warfare*, New York: Hachette Books, 2020;
[27] A Daifullah al-Garni, *Drones in The Ukrainian War: Will They Be an Effective Weapon in Future Wars?* International Institute for Iranian Studies (Rasanah), 2022, pp. 3-5;
[28] NATO, *NATO's Joint Air Power Strategy*, 26 June 2018;
[29] Royal Air Force, *Global Operations*, www.raf.mod.uk/what-we-do/global-operations/. Accessed 14 Mar. 2024;
[30] Gen. J.P. Jumper, *Global Strike Task Force: A Transforming Concept, Forged by Experience*, Aerospace Power Journal, v15 n1 pp. 24-33, 2001;
[31] Gen. D.L. Goldfein, *Eyes to the future*, Air Force Association 2017 Air, Space & Cyber Symposium Remarks, 19 September 2017;
[32] Lt.col. J. Canovas, *Multi-Domain Operations and Challenges to Air Power*, Joint Air & Space Power Conference 2019, ReadAhead – Shaping NATO for Multi-Domain Operations of the Future, The Joint Air Power Competence Centre, 2019;
[33] Lt-Gen. I. Gerhartz, *The Luftwaffe in Multi-Domain Operations*, The Journal of the JAPCC, 30/2020, pp. 9-14.