The Central Research institute
of the Armed Forces of Ukraine

Military Science. Vol. 2 No. 1 (2024)

DOI: 10.62524/msj.2024.2.1.02

A multi-domain operation – a modern view at the forms and methods of military operations adapting to the environment of challenges and threats transformation

Oleh Semenenko
doctor of military sciences, professor
Deputy Head of the Central Research Institute
of the Armed Forces of Ukraine for scientific work
03049, 28B Povitroflotskyi prospect, Kyiv, Ukraine
ORCID: 0000-0001-6477-3414

Volodymyr Koval
candidate of military sciences, senior researcher,
Deputy Chief of the General Staff of the Armed Forces of Ukraine,
03168, 6 Povitroflotskyi Prospect, Kyiv, Ukraine
ORCID: 0000-0002-6209-6779

Oleksandr Vodchyts
candidate of technical sciences, docent
Head of the department
Department of military training National Aviation University
Kyiv, Ukraine
ORCID: 0000-0002-3294-7632

Yuzef Dobrovolskyi
candidate of technical sciences, associate professor, senior researcher
Deputy Head of the Department of Academic Affairs
Department of military training National Aviation University
Kyiv, Ukraine
ORCID: 0000-0002-1077-1402

Abstract. Relevance of the article is due to the fact that Ukraine is currently faced with an operational response to hybrid threats from russia problem of, that include not only military aspects, but cyber security, information warfare, disinformation, non-military measures and other non-traditional methods of warfare also. One of the modern approaches to adopt the forms and methods of Defense Forces (Armed Forces) of Ukraine application of the to the conditions of the development of crisis situations of a military nature the transition to planning and conducting multi-domain operations, i.e. the simultaneous combination of actions in several spaces (domains) at once may be considered. The use of multi-domain operations technology is considered one of the ways to counter the enemy's hybrid threats effectively today. Therefore, the main goal of the article is to reveal the theoretical and practical essence of planning and conducting multi-domain operations, as well as the peculiarities of their organization and implementation. The main methods of research are methods of analysis and synthesis, deduction and induction. The main results of the article are what is defined in it: key features of a multi-domain space military operations conducting; basic aspects of planning and carrying out multi-domain operations; main measures for the preparation and implementation of

multi-domain operations; modern features of the transformation and prospects for adapting the forms and methods of military operations conducting by the Armed Forces of Ukraine in the multi-domain space. The materials of the article can be useful to the leaders of the Armed Forces of Ukraine at the operational and strategic levels, as well as to scientists and researchers in the barnches of research on issues related to the Armed Forces of Ukraine use and ensuring the military (national) security of the State.

Keywords: military operations, domain, use of armed forces, armed conflict, multi-domain operation, multi-domain space, armed aggression, hybrid war, national security, forms and methods of conducting military operations, russian-Ukrainian war, State Defense Forces.

"Technology is the only weapon that can win modern warfare" – Eric Schmidt

Introduction

The research and publications on the topic of the Defense Forces (DF) of Ukraine application forms and methods adaptation to modern challenges and threats of a global nature analysis is a key stage in the development of strategies and tactics in the field of national security. The topic of adaptation of the Ukraine's DF forms and methods of application of to modern challenges and threats became especially relevant during the active phase of the russian-Ukrainian war, that began since February 24, 2023. The Armed Forces (AF) and other components of the DF of Ukraine were forced to look for ways to adapt to new realities and improve strategies for responding modern challenges and threats (Donald M. Snider, & Lewis Sorley, 2016), (Matthew Kroenig, 2018), (Pylypenko, O., & Bazar, O., 2015), (Sun Tzu, approximately V century BC), (Carl von Clausewit., 1832), (Shust, V., & Pavelko, A., 2018), (lesson Shenanigans – Kenyan Hybrid Warfare), (Election Shenanigans – Kenyan Hybrid Warfare), (Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009). During this period, there was a need for an operational response to hybrid threats from russia, covering not only military aspects, but also cyber security, information warfare, disinformation, non-military measures and other non-traditional methods of warfare.

The experience of the ongoing war in Ukraine and in the Middle East (the Arab-Israeli war) analysis results show that current research on the adaptation of the forms and methods of DF applying to conduct of modern warfare subject should be clearly focused on the main aspects, namely: evaluation of effectiveness the use of troops (forces) taking into account modern aspects of the use of innovative technologies; ensuring cyber security; improvements in military doctrine and strategic planning; the development of international cooperation in confronting the aggressor country to ensure stability and security not only in the region, but also in the context of a global scale.

Today, it becomes clear that one of the key areas of research is the optimization of strategies for adaptation of the DF to hybrid threats, which combine military, informational, cybernetic, non-traditional (non-standard) and non-military aspects. It is also important to study the possibilities of introducing innovations in military technologies and tactics of military operations, taking into account modern requirements and the realities of the geopolitical situation. The further development of research is aimed at improving strategies for military training and education, as well as developing effective mechanisms for interaction with other components of national security and other countries, unions, blocs to ensure their own security.

The results of such studies analysis will contribute to optimizing the use of resources and increasing the efficiency of the defense system development under the conditions of modern geostrategic challenges.

Materials and Methods

The forms and methods of the DF of Ukraine application to the modern, transformed environment of challenges and threats (the environment of conducting military operations) ways of adapting study will allow to reveal the main patterns and trends of the further development of the defense sphere of Ukraine, to develop strategies for adapting and improving the Armed Forces to the changing conditions of the situation, and will also contribute increasing the effectiveness of national security in crisis situations (Donald M. Snider, & Lewis Sorley, 2016), (Matthew Kroenig, 2018), (Pylypenko, O., & Bazar, O., 2015), (Sun Tzu, approximately V century BC), (Carl von Clausewitz,1832), (Shust, V., & Pavelko, A., 2018), (lesson Shenanigans – Kenyan Hybrid Warfare), (Election Shenanigans – Kenyan Hybrid Warfare), (Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009), (John, R., & Davis, Jr., 2013), (Horbach, V., 2017), (Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O., 2023), (Portnov, A., 2017), (Abroskin, I., 2022), (New technologies: changing the nature of irregular warfare, 2020), (Sungurovskyi, M., & Gavrilyuk, O., 2019), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022), (Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K., 2021). As a result of the analysis, it became clear that this topic is of great importance for the development of military strategy, tactics, organization and structure of the Armed Forces (Defense Forces), the definition of national security strategies, and also helps to determine the key aspects of the study, namely:

historical examples and cases of adaptation of military strategies and tactics to crisis situations study. For example, analysis of military strategies changes in during World Wars, Cold War conflicts, etc.;

the study of how the development of new technologies affects the capabilities and methods of the military force use, which may involve analyzing the impact of drones, cyber weapons and other innovations on military activities;

the study of how geopolitical changes in the world affect the strategy and tactics of military operations. Adaptation may be necessary due to the changes in enemy forces and means, areas of influence and other factors;

the influence of the social context on the development of military strategies analysis. For example, how society reacts to armed conflicts and how this affects decision-making by the military leadership;

the impact on the adaptation capabilities of the armed forces (defense forces) of the economic restrictions study. Financial restrictions may affect the development of new weapons systems and military equipment, as well as technologies;

the impact of international relations and diplomacy on military strategies and adaptation possibilities, etc study.

the forms and methods of DF of Ukraine application to the transformed environment of challenges and threats adaptation requires a comprehensive approach and careful analysis.

Results

One of the modern approaches to the Ukraine's DF forms and methods application adaptation to the conditions of the development of crisis situations of a military nature of can be considered the transition to multi-domain operations (MDO), that is, a simultaneous combination of actions in several spaces (domains) at once. The use of multi-domain operations is a way to counter hybrid threats from the enemy.

The multi-domain operation is a modern view at the forms and methods of conducting military operations transformation, focused on complex tasks solving in a changing geopolitical environment.

This approach takes into account the importance of integration and synergy in-between different areas of military activity, as well as other important factors. The main aspects of this modern approach include (Election Shenanigans – Kenyan Hybrid Warfare), Menacing Malware Shows the Dangers of Industrial System Sabotage), (Gorbulin, V., 2017), (Daniel T. Lasica, 2009), (John, R., & Davis, Jr., 2013), (Horbach, V., 2017), (Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O., 2023), (Portnov, A., 2017), (Abroskin, I., 2022), (New technologies: changing the nature of irregular warfare, 2020), (Sungurovskyi, M., & Gavrilyuk, O., 2019), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022), (Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K., 2021):

integration of domains. MDO considers the role of land, sea, air, cyberspace and space as interdependent components, where actions in one domain can affect others and vice versa. Integration of these domains allows creating more effective and flexible strategies;

use of technology. MDO actively implements advanced technologies, such as artificial intelligence, cyber defense, autonomous systems and others, to increase the accuracy, efficiency and speed of conducting operations;

flexibility and adaptability. Modern threats and conflict scenarios can change dramatically, and the MDO makes it possible to adapt more quickly and flexibly to new conditions, providing an effective response to various challenges;

synergy with other areas. Outside of military activities, the MDO can interact with economic, political and other aspects, contributing to the creation of an overall strategy to achieve national and international goals;

information management and reporting. MDO requires a high level of information management to make informed strategic decisions and ensure effective control over operations.

In general, MDO is a modern approach to warfare aimed at optimizing the use of resources, increasing efficiency and reducing risks in a high-tech warfare environment.

A multi-domain operation is a military strategy that involves the integration of actions and resources in various military and civilian spheres (domains) to achieve a comprehensive strategic effect. Domains can include land, sea, air, space, information and electromagnetic spaces (Fig. 1).

Main multidomain spaces:

Land. Territorial operations on the land surface, including on land and the coast;

Sea. Operations in maritime space, as well as on the surface and under water;

Air. Military activities in the air space and in the atmosphere;

Space. Use of space resources, in particular satellites, to provide communication, intelligence and navigation;

Information and Cyberspace. Use of information technologies and networks for obtaining, processing and transmitting information.

Modern multi-domain operations are defined by a high degree of integration and cooperation

between the armed forces and other components of society. Information power and cyberspace have gained great importance, because conflicts can unfold not only in physical, but also in virtual space.

The main activities for the preparation and implementation of the multi-domain operations include:

integration and coordination by ensuring effective interaction between forces and assets in all domains;

information dominance, that is ensured by the use of information superiority, including cyberspace, for control and manipulation;

technological advantage, that is provided by the use of the advanced technologies in the fields of intelligence, communication, automation and weapons;

conducting regular training and simulations to increase the level of training and try different scenarios;

creation of the flexible command and control structures for quick response to changes in the combat environment, etc.

Multi-domain operations are becoming an increasingly important aspect of strategic planning as modern military operations are increasingly complex and integrated (Shust, V., & Pavelko, A., 2018), (Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O., 2022). Modern features of conducting military operations in the multi-domain space are determined by the wide use of various technologies and strategies covering several different domains. The table 1 shows several key features of conducting military operations in a multi-domain space with their characteristics.

The transformation of the forms of the military operations conducting in the land domain contains numerous aspects that reflect new requirements, technological and strategic changes in the modern military sphere.

The new technologies and strategies development occurs in the context of changes in the nature of threats, the geopolitical environment, and sociocultural factors.

The application of the latest technologies, such as unmanned systems, artificial intelligence, cyber weapons and smart military systems is one of the key aspects of the transformation. These technologies make it possible to increase the accuracy and efficiency of operations, as well as reduce risks for military personnel. Strategic changes consist in rethinking of the military doctrine and tactical approaches to ground operations. Increasing emphasis on hybrid warfare, cyber security, and responding to new forms of threats such as terrorism and non-standard combat scenarios are becoming important parts of the strategic rethink. In particular, it becomes important to integrate various types of troops and means of warfare to create more flexible and comprehensive strategies. Particular attention is paid to the development of mobility, communication system and information power to ensure a quick and coordinated response to modern threats. In general, the transformation of warfare on land reflects the need to innovate and adapt to changes occurring in the modern military environment to ensure national security and global stability.

The transformation of warfare in the airspace is taking place in the context of various technological and strategic changes that define new requirements and capabilities for the Air Force. In connection with the emergence of advanced technologies and the evolution of strategies, the Air Force is rethinking its role, moving from traditional conflicts to modern forms of military operations. Technological changes involve the development of new types of aircraft, the use and development of unmanned (robotic) systems, and the introduction of artificial intelligence in air operations. These technologies contribute to increasing the accuracy, maneuverability and intelligence of the Air Force.



Figure 1. Modern features of the Armed Forces of Ukraine transformation and prospects for adapting the forms and methods of military operations of conducting in the multi-domain space

The presented military operations in a multi-domain space conducting features are determined by rapid technological development and the need to adapt to modern challenges in the global military environment.

Table 1. The multi-domain space military operations conducting key features

No	Features	Characteristic	Importance for the transformation of military operations
1	Integration and interaction	Ensuring effective interaction and integration of various types of forces, i.e. land, sea, air, space and information space.	Synergy of actions in all domains, which allows more effective use of various military and civilian resources.
2	Digital warfare and cyberspace	Conducting conflicts in cyberspace and using digital technologies to wage a war.	Attacks on information systems, cyberespionage, influence on communication networks are becoming an integral part of military operations.
3	Mass use of drones	Large-scale use of unmanned systems for reconnaissance, attacks and various missions in all domains.	Increasing efficiency, reducing risks to life, but also new challenges arise, such as the danger of drone attacks.
4	Hybrid war	The use of various methods, including military, informational, economic and political, to achieve strategic goals.	Applying a combination of traditional and non-traditional methods to obtain benefits.
5	Hypersonic means and anti-weapon countermeasures	Hypersonic means and systems development to counter hypersonic strikes.	Increasing the speed and complexity of weapons, as well as developing means of countering these attacks.
6	Satellite systems and space domains	Use of space systems for reconnaissance, navigation, communications and warfare.	Ensuring geostationary superiority and responding to challenges in the field of anti-satellite countermeasures.
7	Hybrid management and artificial intelligence	Use of artificial intelligence systems for decision-making and automation of combat processes.	Increased responsiveness and adaptability, but with associated ethical and security challenges.

The main aspects of the transformation of the forms and methods of conducting military operations are given in the table 2 and in the fig. 1.

Table 2. The forms and methods of the military operations conducting transformation main aspects

No	Key features of military operations conducting	Characteristic	Importance for the transformation of military operations
		Domain "Land"	
1	Integration of technologies	Use of modern technologies to increase the accuracy and efficiency of operations on land, such as artificial intelligence, cyber defense, precision weapons.	Improving intelligence capabilities, ensuring accurate and efficient operations.
2	Mobility and expeditionary operations	Mobile military formations development and application and rapid response to changes in the environment concepts.	The ability to move forces and assets quickly to adapt to new threats and challenges.
3	Comprehensive intelligence and surveillance	Use of intelligence from various sources, including drones, satellite systems, intelligence groups.	Providing full-fledged information accounting of the situation for effective decision-making.
4	Hybrid warfare on land	Application of various methods, including informational, economic, cyber and military, to achieve strategic goals.	A new level of complexity in military conflicts that requires flexibility and adaptation.
5	Tube (rocket) artillery and missile systems	Improvement and mass use of artillery and missile systems for accurate hitting of targets on land.	Increasing the range and accuracy of hitting targets.

Table 2 (countinuation). The forms and methods of the military operations conducting transformation main aspects

6	Inventory management and logistics	Application of the latest technologies for efficient management of stocks, supply and logistics.	Increasing the speed and efficiency of moving military formations and material resources.
7	Hybrid threats and countermeasures	Measures to protect against hybrid threats such as terrorism and hybrid attacks.	Increasing the ability to cope with new forms of hostile activity.
8	Training and learning	Application of modern methods of training and simulations to prepare the military for operations on land.	Ensuring a high level of readiness and adaptability of forces.
Domain "Air"			
1	Unmanned aviation and drones	Wide use of unmanned aerial vehicles (UAVs) for reconnaissance, strike and logistics tasks.	Increasing reconnaissance capabilities, reducing risk for pilots, new challenges in the field of cyber defense.
2	Hypersonic aircraft	The use and development of aircraft capable of traveling at the speeds, that are highly exceeding the speed of sound.	Increased speed and unparalleled ability to react quickly.
3	Integration and network operations	Air Force interactions with other domains and the use of network technologies to provide coordination and information sharing.	Improved operational efficiency through improved communication and data sharing.
4	Electronic warfare and cyber defense	The use of electronic warfare for intelligence and support missions, as well as enhancing the cyber defense of the air systems.	Providing protection against electronic attacks and ensuring the integrity of systems.
5	Vertical take-off and landing vehicles and helicopters	Increasing the use of vertical take-off and landing (VTOL) to improve mobility and operational efficiency.	Ability to operate in conditions where access to conventional airfields is limited or impossible.
6	Aircraft capable of autonomous flight	The development of aircraft capable of autonomous flight and performing tasks without the direct control of the pilot.	Improving the effectiveness and capabilities of missions through autonomy.
7	Lots of data and analytics	Using large amounts of data and analytics for decision-making and intelligence at various stages of tasks.	Improving the ability to analyze and use intelligence information.
8	Global presence	Increasing the ability to have a global presence and respond quickly to threats anywhere in the world.	Ensuring rapid response to conflict escalation and security threats.
9	Development of hypersonic technology	Use of hypersonic technologies to create and improve means of conducting military operations in airspace.	Increasing the speed and efficiency of operations.
Domain "Sea"			
1	International security and protection of sea routes	Ensuring the security of sea routes and control over territorial waters to protect against threats and hostile influence.	Preservation of maritime freedom and economic interests.
2	Expeditionary operations and power projection	The ability to project military power over long distances to solve strategic tasks quickly and effectively.	Flexibility and ability to respond to different threats in different parts of the world.
3	Multidomain integration	Interaction with air, land and space for synergy and ensuring integrated operations.	Improving coordination and effectiveness between different domains of warfare.
4	Anti-submarine warfare	Development of means and strategies for detecting and countering underwater objects.	Ensuring the safety of the maritime space and avoiding underwater threats.
5	Means of countering the aerial threats	Development and application of means of combating air attacks for the protection of ships and other objects.	Ensuring security against air threats and increasing defense capabilities.

Table 2 (countinuation). The forms and methods of the military operations conducting transformation main aspects

6	Naval Blitzkrieg and Hybrid Warfare at Sea	Use of hybrid warfare strategies in the maritime environment, including asymmetric and non-standard threats.	Adapting to a variety of threats and conducting operations in a complex environment.
7	Environmental awareness and infrastructure	The ability to conduct military operations, taking into account the impact on the environment and existing infrastructure.	Ensuring sustainable use of maritime space and taking into account environmental aspects of military operations.
8	Global presence and capacity to deliver humanitarian aid	Ensuring the possibility of providing humanitarian aid and the ability to respond to natural disasters quickly.	Use of naval forces to support global humanitarian tasks.
9	Ensuring full security of maritime logistics infrastructure	Measures to protect naval bases, ports and logistics infrastructure from possible threats.	Ensuring long-term operational capability through secure provisioning and support.
Domain "Cyberspace"			
1	Cyber protection and cyber security	Development of measures to protect critical infrastructures and information systems from cyberattacks.	Ensuring stability and security in the information space.
2	Cyber military operations and cyber attacks	Carrying out operations in cyberspace with the aim of causing damage, gathering information or hindering the work of the adversary.	The use of cyber means as a component of military conflict.
3	Information warfare and influence	The use of information means to manipulate public opinion, influence decision-making, and create an image of the enemy.	Directed influence on the information field to achieve military and political goals.
4	Artificial intelligence in cyberspace	Using artificial intelligence to identify and analyze threats, automate cyber defense and implement cyberattacks.	Improving the speed and accuracy of response to cyber threats.
5	Cyber military forces and cyber command	Creation and development of specialized military units for conducting operations in cyberspace.	Ensuring expert qualification and ability to conduct cyber military operations.
6	Cyber special operations and cyber intelligence	The use of cyber means for conducting intelligence, gathering information and implementing special operations in cyberspace.	Carrying out actions in cyberspace for the purpose of obtaining intelligence information and ensuring security.
7	Cyber hybrid threats	The combination of cyberattacks with other types of threats such as information, hybrid warfare and cyber terrorism.	Complication of warfare and increase in the number of potential threat options.
8	International cyber coordination and regulations	Development of international standards, provisions and treaties for cyber military relations regulation.	Ensuring stability and control in cyberspace.
	Training and training of cyber defense forces	Development of training and training programs to ensure high qualification of cyber specialists.	Training the military to operate effectively in cyberspace and respond to cyber threats.
Domain "Space"			
1	Space intelligence and response	Application of satellite systems for reconnaissance, navigation and ensuring the accuracy of military operations.	Ensuring high-quality intelligence and prompt response to changes in the situation.
2	Space communication and signal communications	Use of space systems to ensure continuous and secure communications between military units.	Ensuring effective communication and coordination over long distances.
3	Space defense and anti-satellite means	Development of systems and technologies for protection against attacks on space assets and anti-satellite means.	The normal functioning of space vehicles guaranteeing and protection against enemy interference.

Table 2 (end). The forms and methods of the military operations conducting transformation main aspects

4	Space Armed Forces	The development and use of military systems located in outer space for the implementation of various tasks.	Ensuring military superiority and the ability to conduct operations at various levels.
5	Cooperation in outer space	Development of international cooperation and standards for the use of outer space for peaceful and military purposes.	Reducing the possibilities of conflicts in outer space and joint implementation of projects.
6	Space intercontinental strike means	The use of space means to deliver strikes (carrying out strikes?) over long distances between continents.	Ability to influence strategically and conduct global operations.
7	Space electronic warfare	The use of electronic means of influence in outer space for reconnaissance and enemy interference tasks.	Ensuring the effectiveness of electronic warfare and control over the electromagnetic space.
8	Exploration and navigation in outer space	Use of satellite systems for reconnaissance and navigation to support operations in other domains.	Ensuring the accuracy and reliability of information for conducting military operations.
9	Space ecological consciousness	Consideration of outer space from the point of view of preserving its sustainable functioning and maintaining environmental cleanliness.	Reducing the impact of military operations on the space environment.

Strategic changes reflect a rethinking of the tasks and functions of the Air Force in modern military conflict. There is an increasing emphasis on integration with other types of forces, including cyber and space forces. The strategies also involve adapting to hybrid threats such as cyberattacks and unmanned aerial vehicles. Flexibility, mobility and the ability to adapt to the changing conditions of the theater of operations are key requirements for the Air Force. The development of communications and information technology systems is also important to ensure effective coordination and communication during hostilities. All this indicates the need for a constant innovative approach and a modern definition of the role of air forces in military strategies, in particular, to ensure safety and efficiency in modern combat conditions.

The transformation of the forms of conducting military operations in the "Sea" domain contains a number of key aspects that reflect modern trends, technological development and strategic changes in the maritime military environment. The transformation of the conduct of military operations in the maritime space takes place in the context of changes in geostrategic conditions, technological innovations and the needs of the modern security environment. One of the key aspects of the transformation is the development of new technologies in the field of naval warfare. The use of unmanned vessels, nuclear and hybrid energy systems, effective means of intelligence and communication makes it possible to conduct operations more accurately and provides an advantage in the maritime space. It is important to adapt strategies to changes in geostrategic conditions. Growing competition for resources, the development of the Arctic as a new arena for geostrategic interests, as well as the impact of climate change on sea lanes require new strategies for conducting maritime operations. The conditions of the modern security environment also reflect the need to ensure maritime security, combat transnational threats such as piracy and terrorism, and the ability to effectively interact with other types of military and civilian structures. In general, the transformation in naval warfare is defined by the need to adapt to new challenges and opportunities arising in a changing global context and the development of innovative strategies and technologies to ensure maritime security and the effective conduct of operations in this important domain.

The transformation of warfare in the Cyberspace domain is taking place in connection with the rapid development of technologies and changes in the nature of military threats. The transformation of conducting military operations in cyberspace is determined by rapid technological development and the emergence of new challenges in this area. Adaptability and innovation are becoming key

factors for effective operations in this space. In today's world, cyberspace has become an important field for conducting military operations, as digital technologies have penetrated all spheres of life. Advances in artificial intelligence, cyberattacks, and other aspects of cybersecurity are creating new opportunities for warfare while simultaneously endangering national and international security. Changes in the nature of threats in cyberspace require constant improvement of strategies and technical solutions. In particular, the ability of countries and military organizations to adapt their approaches to new technologies and skills of cyber military threats is important. Cyber security innovation, cyber threat studies, and training of military personnel are becoming critical components to ensure successful operations in this critical space. Given these transformations, it is important to maintain international cooperation and develop cybersecurity standards to create a united line of defense against cyber threats and ensure stability and security in this important military domain.

The transformation of the military operations in the "Space" domain conducting forms is taking place in the context of the rapid development of space technologies and strategic changes in the geostrategic environment. This process involves not only technical aspects, but also the formation of new strategies and tactics aimed at ensuring national security in outer space. With the advent of new technologies such as satellites, space weapons and space intelligence systems, the role of space in the military has become extremely important. Countries are actively working to develop and improve means of space warfare to ensure strategic superiority and control in outer space. At the same time, changes in the geostrategic environment require the adaptation of strategies for warfare in outer space. The growing competition between countries for resources and influence in space makes it urgent to develop and implement effective strategies aimed at preserving national security in this new military domain. In this context, there is a need for international cooperation and the development of international standards for the regulation of space warfare in order to prevent conflicts and ensure stability in space. National and international policy efforts should be directed toward creating balanced and sustainable strategies for warfare in outer space to preserve peace and stability at the planetary level. The transformation of the military operations conduct in outer space is determined by the struggle for control and use of this domain resources, as well as the resolution of issues of international cooperation and environmental sustainability.

The russian-Ukrainian war has showed that the transformation of modern forms and methods of conducting military operations is currently place actively taking as a result of the influence of both the hybridization factor and the technological factor of military confrontation. The main types of operations that characterize the conduct of military operations in the russian-Ukrainian war include point and mass drone strikes, mass and combined unmanned operations, as well as, in order to counter drones, anti-drone operations, etc.

Spot and mass drone strikes have become an important component of modern warfare strategies.

Spot drone strikes are strikes aimed at specific objects or targets in a limited area. Point strikes try to minimize collateral damage and are aimed at specific, often strategically important, objects. Point-of-care drone strikes require precise targeting, high accuracy of strikes, the ability of artificial intelligence to recognize and select targets, and coordination with other systems.

Mass drone strikes are strikes where many drones launch synchronized attacks on large areas or groups of targets. The purpose of such strikes is to maximize the impact and coverage of the territory. Massive drone strikes require a large number of drones, synchronization of attacks, effective communication and control of a group of drones. Algorithms for the distribution of targets are used for optimal coverage of the territory.

The main measures for the preparation and execution of drone strikes include:

intelligence and recognition. It is necessary to have reliable intelligence to accurately identify targets;

technical training. Provide drones with high accuracy, high speed and the ability to evade anti-

aircraft weapons;

communication and management. Provide a reliable control and communication system between drones and operators;

protection against countermeasures. Countermeasures implementation (antiviruses, electromagnetic protection systems, etc.).

It is important to note that the use of drones in military operations should be in accordance with international legislation and rules, and ethical and humanitarian issues may arise in this connection.

A mass drone operation is the coordinated activity of a large number of unmanned aerial vehicles (drones) with the aim of influencing a defined area or objects, often using a significant number of drones to simultaneously attack or perform different tasks.

Massive unmanned operations are a modern approach to conducting operations that can provide great flexibility and efficiency in various situations. Consideration of ethical, legal and security issues is an important aspect when designing and implementing such operations.

A combined unmanned operation is a type of military strategy that uses a combination of different types of unmanned vehicles and their interaction to achieve complex strategic goals. This strategy involves the use of a variety of drones with different functions and capabilities in a single, coordinated operation. Combined Unmanned Operations use different types of drones to maximize efficiency and a wide range of capabilities in different scenarios. Effective planning, technology integration and security are key components of successful implementation of such operations.

An anti-drone operation is a military or civilian activity aimed at detecting, identifying, interacting or neutralizing unmanned aerial vehicles (drones) that may pose a threat to security, privacy or violate laws and regulations. An anti-drone operation requires a comprehensive approach to identify and neutralize potential threats that may arise from the use of drones.

The main characteristics and measures for carrying out the above types of modern operations in various domains are presented in the table. 3.

In today's combat environment, warfare is increasingly dependent on the use of unmanned aerial vehicle, including targeted and massed drone strikes, massed and combined unmanned operations, and counter-drone operations (anti-drone operations).

Multi-domain operations involve interaction and coordination between different domains or areas of activity, such as information security, network communications, data processing, cloud computing, and others. Here are some of the main modern technologies used in a multi-domain operations system:

artificial intelligence (AI): AI is used to automate the decision-making processes, analyze large volumes of data, make predictions, and more. In multi-domain operations, AI can be applied to automate threat response, anomaly detection, and improve overall operational efficiency;

Blockchain: Blockchain technology provides a decentralized and reliable data storage system that can be useful for data security and identity verification in multi-domain operations;

cyber security: cyber security technologies such as network firewalls, intrusion detection systems (IDS), access management systems (AMS), data encryption and many others are used to protect multi-domain operations from cyberattacks;

cloud computing: cloud services provide the ability to store and process data in different domains through virtual computing resources, which facilitates data exchange and collaboration between different domains;

Internet of Things (IoT): IoT devices enable the collection and exchange of data between various objects and systems. In multi-domain operations, they can be used to collect data from different domains and provide their analysis and management;

process automation: the use of various automation tools, such as robots with artificial intelligence (Robotic Process Automation, RPA) or automated control systems, makes it possible to optimize processes in multi-domain operations and reduce the level of errors;

data analytics: Data analysis technologies such as machine learning, natural language processing (NLP) and others help extract valuable insights from large volumes of data collected from different domains to support decision-making in multi-domain operations.

Table 3. Combined and massive unmanned operations and anti-drone operations conducting main characteristics and measures

Characteristic	Content of the main activities
Massive unmanned operation	
Massiveness	Number of drones: Mass drone operations involve a significant number of drones that can be used for a wide range of tasks.
Various functions	Attacks: Depending on the operator's needs, drones can perform air or ground attacks. Intelligence and Reconnaissance Tasks: Drones can be used for intelligence gathering and data transmission.
Coordination and communication	Control systems: There is a need for reliable and secure control systems to effectively coordinate the actions of a large number of drones. Communication networks: creation of reliable communication networks for transmitting commands and receiving information in real time.
Automation and artificial intelligence	Autonomy: Some mass operations may involve autonomous drones that independently perform tasks based on programming and analysis of the surrounding environment. Artificial Intelligence: Using artificial intelligence algorithms to identify and analyze targets and optimize decisions in real time.
Security and challenges	Defense against interference: development of means of protection against electromagnetic interference and other threats to unmanned systems. Information security: protection against hacker attacks and ensuring the confidentiality and integrity of data.
Application in various fields	Military use: Mass drone operations are widely used by the military to carry out attacks, reconnaissance and other tasks. Civilian use: applications in civilian areas such as natural disaster intelligence, agricultural sector, etc.
Combined unmanned operation	
Various drones	Tactical aircraft: drones designed for close-range attacks and reconnaissance. Strategic Drones: Drones capable of long-range operations and large-scale missions. Reconnaissance drones: designed for information gathering and reconnaissance without interfering in the combat space.
Integration and coordination	Joint communications: ensuring effective information exchange between different types of drones and command centers. Control systems: development of a single control system to coordinate the entire network of unmanned aerial vehicles.
Automation and artificial intelligence	Autonomy Systems: Using Autonomy Technologies to Make Independent Decisions by Drones in Real Time. Artificial intelligence: implementation of artificial intelligence algorithms for analysis and interpretation of received data and automation of decision-making processes.
Distribution of tasks	Drone Specialization: Using drones with various specialized capabilities to effectively perform specific tasks. Interaction between classes: ensuring the interaction and synchronization of the operation of different classes of drones.
Adaptability and flexibility	Responsiveness: the ability of a drone network to adapt to changes in the combat environment and shift focus to the most important tasks. Backup Mechanisms: Implementation of security measures and backup mechanisms to avoid losses in case of loss of individual drones.

Table 3 (end). Combined and massive unmanned operations and anti-drone operations conducting main characteristics and measures

Safety and ethics	Cyber threat protection: ensuring network security and protection against cyberattacks. Ethical aspects: consideration of ethical principles in the use of unmanned systems in military operations.
Anti-drone operation	
Detection and recognition	Using radars, thermal imaging sensors, optical cameras and detection systems to recognize drones in the air. Consideration of various characteristics of drones, including size, speed, shape and other parameters.
Identification and classification	Using identification systems that can identify the type and model of drones. Application of databases for classification of drones and recognition of their manufacturers.
Interaction and interception	Using crash signals to disrupt drone operation and loss of control. Use of interception systems, such as radio frequency or other methods of jamming the drone's signal.
Physical intervention	Using means of physical interference to destroy or operate drones, such as using lasers or other energy systems.
Protection against cyber threats	Preventing the possibility of hacking and taking control of drones. Protection against attacks on infrastructure and management systems.
Intelligence and counterintelligence	Carrying out constant monitoring of the airspace to identify potential threats. Use of drones or other means to detect and recognize drones.
Use of technical means	Installation of anti-drone systems such as radars, signal jammers and interceptors. Application of technical means for detection and blocking of unmanned aerial vehicles.
Staff training and education	Training of personnel for effective interaction and response to various scenarios of anti-drone operations. Use of simulators and training grounds for training.
Legislative measures	Establishing rules and restrictions on the use of drones in certain areas or at a certain distance from objects that need protection.
Coordination with airports and air traffic control	Cooperation with airports and air services to control drones to identify and eliminate potential threats.
Ensuring security	Installation of defense systems against cyberattacks and provision of appropriate security measures for anti-drone systems.

These technologies can be used separately or in combination to create integrated management systems and optimize multi-domain operations.

The study of modern technologies in the system of multi-domain operations is of great importance during a conflict such as the russian-Ukrainian war for several reasons:

ensuring security and defense capability: thanks to the use of advanced technologies in the multi-domain operations system, countries have the opportunity to ensure more effective control over their territorial interests and reduce the risks of military threats;

cyber security and information warfare: Cyber security and information warfare are given a lot of attention in modern conflicts. Thanks to the research of the latest technologies, countries protect their information resources and infrastructure from cyberattacks, as well as carrying out their own operations in this area;

efficient use of resources: It is possible to optimize the use of resources that may be limited during a conflict thanks to the development and implementation of modern management technologies;

international cooperation: the modern technologies in the system of multi-domain operations study may contribute to cooperation between countries working together to solve modern security challenges;

moral and ethical aspect: the use of advanced technologies also requires discussion of moral and ethical issues that may arise as a result of their implementation, in particular, in the field of automation and robotization of military operations.

Therefore, the modern technologies in the system of multi-domain operations study during the ongoing russian-Ukrainian war is critically important for ensuring national security, effective use of resources, and successful conduct of military operations.

Discussions

The main prospects for the forms and methods of military operations conducting transformation in the modern combat environment include:

deep, dynamic development of technologies: the prospects include the continuous development of technologies in the field of unmanned aviation, the improvement of artificial intelligence systems and the increase of the autonomy of drones;

integration with other technologies: interaction of unmanned systems with cybernetic and other modern technologies to create highly effective and complex military strategies;

ethical and legal aspects: the production and use of drones requires attention to ethical and legal issues, particularly those related to privacy, security and liability.

In general, the introduction of unmanned technologies opens up new opportunities for conducting military operations, providing a more effective and safer strategy compared to traditional methods. At the same time, new challenges arise related to protection against anti-drone threats, regulation of use and development of ethical standards in the military sphere.

Conclusion

The research and implementation of modern technologies in the system of multi-domain operations are of great strategic importance in the context of the ongoing russian-Ukrainian war. The security challenges, including cyber threats, hybrid attacks, and information warfare, that are given today's, the effective use of advanced technologies is becoming a key aspect for ensuring national security and defense capability.

The research in this field helps countries strengthen their defense capabilities, improve the protection of critical infrastructure, respond effectively to threats, and ensure the safety of their citizens. In addition, it promotes international cooperation and exchange of experience between countries to counter modern security challenges.

The investment in the research of modern technologies in the system of multi-domain operations, in general, is a critically important element of the strategy of ensuring national security and successful conduct of military operations under the conditions of the modern geopolitical environment.

Recommendations

Multi-domain operations, that cover different types of warfare and use a variety of military and non-military means, are becoming an important part of a strategic planning in today's combat environment.

We offer the basic recommendations for the prospects for the development of such operations formation, taking into account the experience of the russian-Ukrainian war and the Israeli war against Hamas in 2023.

1) Integration of various types of troops. Development and improvement of communication and communication systems between the components of the armed forces, including land, air, sea and

space components, which will contribute to more effective coordination and joint work between various branches of military activity.

2) Information warfare and cybernetic aspects. The growing role of cyber operations and information warfare in multi-domain conflicts. Establishing cyber measures to affect enemy communications systems, electronic systems and infrastructure.

3) Use of unmanned technologies. Intensive development and use of unmanned aerial vehicles in all areas of military activity, including reconnaissance, strikes, transportation and medical assistance. Effective use of drones can provide an advantage in combat operations.

4) Synergy with special operations forces. The importance of the special forces that can perform a variety of tasks in different areas of the combat zone. The operational mobility and flexibility of such forces make them a key component of multi-domain operations.

5) The technologies of hybrid warfare and modern conflicts application. Consideration of hybrid threats, that include not only military, but also political, economic and other aspects. Adapting strategies to the specifics of hybrid warfare and using conflict experience to build more complex strategies.

6) Development of innovations in technologies and weapons. Application of advanced technologies such as artificial intelligence, pattern recognition and cyber-physical systems. Improvements in weapons and equipment to ensure accuracy, maneuverability and reliability in a multi-domain conflict.

7) Taking into account the geopolitical aspect and international cooperation. Development of strategies that take into account geopolitical realities and the possibility of international cooperation in multi-domain operations. Joining the efforts of different countries can become a key element for ensuring stability and countering threats.

8) Development of humanitarian aspects. Consideration of humanitarian aspects in planning and conducting operations. Balanced strategies that take into account the needs of local populations can contribute to saving lives and restoring stability after conflict ends.

9) Application of the non-military methods of confrontation. Development and implementation of the non-military methods of confrontation, such as diplomacy, economic pressure and other non-aggressive strategies to achieve the goal without escalating the conflict.

10) Active use of asymmetric warfare technologies. Taking into account the possibilities of asymmetric threats and warfare techniques. Optimizing strategies for fighting small but technologically advanced opponents.

11) Ensuring cyber security. The growing focus on cyber security in multi-domain operations, given the possibility of cyberattacks on critical military and civilian infrastructure.

12) Emphasis on training and preparation. Development of education and training programs for military and civilian personnel aimed at understanding and effective use of various means and methods in multi-domain operations.

Considering these aspects, multi-domain operations become necessary for effective warfare in today's world, especially during conflicts where a variety of technologies are used and flexible and adaptive strategies are defined. The abovementioned main aspects of multi-domain operations take into account the dynamics of the modern combat environment and develop in accordance with modern challenges and trends in the military sphere. Multi-domain operations require the integration of various means and strategies to achieve a comprehensive and effective response to modern threats.

Acknowledgments

The authors declare that they have no competing interests in the subject of the article.

References

1. Donald M. Snider, & Lewis Sorley (2016). *Understanding War: An Annotated*

Bibliography. Washington, DC. Strategic Studies Institute, US Army War College. P. 157.
2. Matthew Kroenig (2018). *The Logic of American Nuclear Strategy: Why Strategic Superiority Matters*. Oxford. Oxford University Press. P. 312.
3. Pylypenko, O., & Bazar, O. (2015). *Military art of Ukraine: history and modernity*. Kyiv. Criticism. C. 256.
4. Sun Tzu. *The Art of War*. (approximately V century BC). Ancient China.
5. Carl von Clausewitz. (1832). *On War*. Berlin. Dümmlers.
6. Shust, V., & Pavelko, A. (2018). *Military strategy: theory and practice*. Kyiv. NUOU. P. 320.
7. lesson Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DMZJ893.
8. Election Shenanigans – Kenyan Hybrid Warfare (Book). ASIN B08DGP72MH.
9. Menacing Malware Shows the Dangers of Industrial System Sabotage.
10. Gorbulin, V. (2017). What kind of Phoenix will be born from the ashes of the global hybrid war? 3d of November. *Mirror of the week*.
11. Daniel T. Lasica. (2009). Strategic Implications of Hybrid War: A Theory of Victory. *School of Advanced Military Studies*.
12. John, R., & Davis, Jr. Defeating Future Hybrid Threats. (2013). *Military Review*, September-October 267. 7. Armed Forces Journal: Hybrid vs. compound war (eng.) (1.10.2009). http://armedforcesjournal.com/hybrid-vscompound-war/
13. Horbach, V. (2017). *Military strategy of Ukraine*. Kyiv. NUDU. P. 256.
14. Semenenko, O., Vodchyts, O., Tolok, P., Mytchenko, S., Hetman, A., & Tarasov, O. (2023). The main theoretical and practical aspects of conducting proxy wars and hybrid wars in the modern global geopolitical and security environment: history, theory, practice, forms and methods, experience for Ukraine. *Social development and security*, No. 13 (3), pp. 1–23. https://doi.org/10.33445/sds.2023.13.3.1
15. Portnov, A. (2017). *Ukrainian wars: from the collapse of the Soviet Union to modern conflicts*. Kyiv. KM-Buks. P. 312.
16. Abroskin, I. (2022). *Hybrid warfare: threats and responses*. Kyiv. Yakabu Publishing. 305 p.
17. New technologies: changing the nature of irregular warfare. (2020). Modern Diplomacy. https://moderndiplomacy.eu/2020/05/11/emerging-technologies-changing-nature-of-irregular-warfare.
18. Sungurovskyi, M., & Gavrilyuk, O. (2019). *Military reform in Ukraine: strategic challenges and solutions*. Kyiv. Institute of National Security Problems named after I. Yavornytskyi. P. 160.
19. Semenenko, O., Koverga, V., Ostapenko, O., Kravchenko, Yu., Mytchenko, S. & Tarasov, O. (2022). Russia's military expenditures analysis and their structure in the period 2010-2022 (some aspects of the influence and consequences of the russian-Ukrainian war for Ukraine). *Social development and security*, No. 12 (5), pp. 116–129. https://doi.org/10.33445/sds.2022.12.5.11.
20. Semenenko, O., Voronchenko, I., Moskalenko, I., Abramova, M., & Kharitonov, K. (2021). A methodological approach to assessing the ability of the national economy to ensure a sufficient level of defense capability. *Social Development and Security*, 11(5), 133–145. https://doi.org/10.33445/sds.2021.11.5.13
21. Solomytskyi, A., Semenenko, O., Onofriychuk, P., Slyusarenko, M., Baranov, S., & Mitchenko, S. (2022). Forecasting the risk of armed conflict based on the analysis of military costs. *Social Development and Security*, 12 (1), 164–

174.https://doi.org/10.33445/sds.2022.12.1.15

22. Semenenko, O., Deinega, O., Voronchenko, I., Borysyuk, S., Mytchenko, S., & Taran, O. (2021). To the question of the transformation of the forms and methods of military operations in the conditions of hybrid wars. *Social Development and Security*, 11 (2), 256–271.https://doi.org/10.33445/sds.2021.11.2.22
23. Wojtowicz, T., & Król, D. (2019). Multi-domain battle. The new doctrine of the Armed Forces of the United States. *Zeszyty naukove akademii sztuki wojennej*. Vol. 112, No. 3. P. 64–78.
24. Semenenko, O., Taran, O., Mytchenko, S., & Butenko, R. (2022). Recommendations on the forms and methods of use of the Defense Forces of Ukraine adapting to the conditions of conducting military operations, taking into account the influence of the hybridization factor. *Collection of sciences. pr. CSRI of the Armed Forces of Ukraine*, 2 (101), 16–31.