ROMANIAN MILITARY THINKING

APPROACHES TO THE CONCEPT OF *"MULTI-DOMAIN OPERATIONS"* IN THE DOCTRINAL VISION OF NATO AND ITS MAIN STRATEGIC COMPETITORS

Colonel Senior Instructor Iulian-Radu MONORANU, PhD Student
"Nicolae Bălcescu" Land Forces Academy, Sibiu
DOI: 10.55535/RMT.2025.1.01

As the global security landscape becomes increasingly complex due to the intensification of global competition and the growing interdependence among various operational domains – land, maritime, air, space, and cyber – key actors are adapting their military doctrines to exploit these interactions and gain strategic advantages. This article examines the approaches to the concept of multi-domain operations (MDO) from the doctrinal perspective of NATO's main strategic competitors. The study provides a comparative analysis of the multi-domain operational concepts adopted by major powers, highlighting both the similarities and differences in their strategic approaches. By reviewing doctrinal documents, analysing lessons learned from conflicts and military exercises, as well as other relevant sources, the article identifies the factors influencing the evolution of these doctrines and their impact on global security dynamics. The conclusions suggest that NATO's continuous adaptation to these doctrinal changes is essential for maintaining a position of strategic superiority in an ever-evolving security environment.

Keywords: multi-domain operations; Russia; weapons technology; China; disinformation;

INTRODUCTION

Developing a new approach to military strategy requires a thorough understanding of both the current and future operational environment, as well as its evolution from past conflicts. Over the past two decades, as NATO member militaries have shifted their doctrines and resources toward counterinsurgency operations, allowing their high-intensity warfare capabilities to atrophy, several powerful state competitors have escalated their aggressive behaviour. By asserting their dominance in the operational environment, these actors have signalled a return to a new era of great power competition. The likelihood of military conflict against a near-peer adversary or a regional actor of a similar rank to the USA or NATO has increased significantly, imposing the need to rapidly focus on effective competition in all areas and across the full spectrum of military operations.

The likelihood of military conflict against a near-peer adversary or a regional actor of a similar rank to the USA or NATO has increased significantly, imposing the need to rapidly focus on effective competition in all areas and across the full spectrum of military operations.

A comparative analysis of NATO's Strategic Concept (2022) and the US National Defense Strategy shows a coherent position on the definition of common threats and the identification of the main strategic adversaries of the Western powers. The USA points out that over the past decade, we have witnessed Russia's increasingly aggressive and retaliatory actions, China's military rise and economic emergence, an increasingly threatening North Korea and an unscrupulous Iranian regime. Each of these adversaries aims to alter the world order in their favour and challenge the strategic interests of Western states (US DoD, 2022, pp. 2-7). Following the outbreak of the war of aggression against Ukraine, NATO positions Russia as posing *"the most significant and direct threat to the security of allies"*, judging that it is attempting *"to fundamentally change the Euro-Atlantic security architecture"*. At the same time, the Alliance condemns *"the coercive and ambitious policies of the People's Republic of China, its hostile rhetoric, disinformation and exertion of economic influence to create strategic dependencies"*,

as well as the deepening of its *"unrestrained"* strategic partnership with Russia. Also, the *"further development of nuclear and ballistic missile programs"* by Iran and North Korea while *"providing direct military support to Russia to fuel the war against Ukraine"* remains a permanent threat to NATO (MAE, 2024).

The strategic inter-state competition, highlighted by the ongoing armed clashes in the Euro-Atlantic area and the Middle East, as well as by the tensions in the Indian Ocean and Asian area, is mainly driven by the growth of military arsenals and supported by unprecedented technological development that ensures rapid and continuous integration of all areas of warfare. Advancements in weapons technology, sensors, communications, and information processing have significantly enhanced the lethality of military operations. Adversaries now possess the capability to detect, track, and target military forces across the full depth of the extended battlefield, particularly in emerging domains such as cyber, information, and space. They seek to gain a strategic edge by integrating land, air, sea, cyber, and space-based strike capabilities. Furthermore, in the information environment, adversaries engage in intense competition, frequently employing propaganda, disinformation, misinformation, and deception to manipulate perceptions and create a distorted or ambiguous representation of reality. All the mentioned aspects represent the new coordinates of contemporary warfare that are changing the way of fighting and call for the adoption of new concepts of operation.

The strategic inter-state competition, highlighted by the ongoing armed clashes in the Euro-Atlantic area and the Middle East, as well as by the tensions in the Indian Ocean and Asian area, is mainly driven by the growth of military arsenals and supported by unprecedented technological development that ensures rapid and continuous integration of all areas of warfare.

In this article, through the investigation and analysis of official documentary sources, together with the comparative analysis of the results of case studies and lessons learned from recent military operations or exercises, we aim to highlight the key principles, similarities and differences in the doctrinal approach to Multi-Domain Operations (MDO) at the Alliance level and the main declared strategic adversaries – Russia, China, Iran and North Korea.

The findings will point to possible directions for analysing capabilities and estimating the actions of potential adversaries, while calling for the continued adaptation of the Alliance to maintain a position of strategic superiority in today's changing security environment.

USA AND NATO APPROACHES TO THE CONCEPT OF MULTI-DOMAIN OPERATIONS

The accelerated technological advances in all fields, the development of space systems, autonomous robotic systems, the information and communications revolution have fundamentally altered the way military organizations prepare to wage war. Today's armed forces face the challenge of adapting their doctrine and tactics at an accelerated pace to the rapidly changing nature of future conflict. For the USA and NATO, the resurgence of great power competition, the advancement of anti-access/area denial (A2/AD) capabilities by peer adversaries such as Russia and China, and their strategic competition below the threshold of armed conflict across multiple regions have been the primary drivers behind the development and implementation of the MDO concept as an effective response. Seeking to counter the successful application of Allied doctrines in operations in Iraq and the Balkans, strategic adversaries have focused their efforts on building up high-battle, multi-layered engagement capabilities that deter proximity and provide so-called Anti-Access/Area Denial (A2/AD) *"bubbles"* with the ultimate goal of preventing freedom of manoeuvre by Western enemy military forces in all domains, in areas of previously unchallenged superiority. These aspects immediately increased the US military's concern about the *"inability to make direct contact with the enemy, destroy him, conquer and secure the terrain, and then consolidate gains"* (Dwight, 2023, p. 2). Thus, it was necessary to rethink doctrine to combat in particular the enemy's layered capabilities of holding at a distance (with integrated fire support and air defence systems) in order to create windows of opportunity for freedom of manoeuvre for the assembled forces.

For the USA and NATO, the resurgence of great power competition, the advancement of anti-access/area denial (A2/AD) capabilities by peer adversaries such as Russia and China, and their strategic competition below the threshold of armed conflict across multiple regions have been the primary drivers behind the development and implementation of the MDO concept as an effective response.

The new concept has been crystallizing since 2014, with Russia's invasion of Crimea being a powerful catalyst for American military and civilian experts in the US Department of Defense, who were convinced that the threat of an invasion of US or allied territory by an advanced military enemy with similar capabilities would seem plausible and difficult to defend against. Combining successful elements of earlier concepts, American thinkers base the new concept on the doctrinal principles of *air-land battle*, applied to an expanded and integrated battlespace that involves incorporating new domains such as space

and cyber, the electromagnetic spectrum and the information environment in addition to the traditional land, sea and air. At the same time, the term *"battle"*, which has tactical connotations applicable only to armed conflict, is replaced by *"operations"*, a term specific to the operational and strategic level, which is intended to address both the competitive and conflict phases and to better describe both joint force actions in all areas and inter-allied and inter-agency actions. An evolution of joint operations, the MDO concept – formalized in the FM 3-0 Operations doctrine – integrates capabilities across all domains to *"create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains"* during competition, crises, and armed conflicts (US Army, 2022). MDO extends beyond the operational level, requiring the coordination of distinct forms of manoeuvre across five domains while engaging agencies, intergovernmental organizations, and allied forces to develop asymmetric strategic responses on a global scale. Given the speed and operational reach of advanced weapon systems, as well as the complexities of global logistical support chains, such joint operations can no longer be restricted to clearly defined geographical areas (Lund-Hansen, Reilly, 2024).

An evolution of joint operations, the MDO concept – formalized in the FM 3-0 Operations doctrine – integrates capabilities across all domains to "create and exploit relative advantages that achieve objectives, defeat enemy forces, and consolidate gains" during competition, crises, and armed conflicts.

Three fundamental principles define the new operational concept: the positioning of joint and inter-allied forward-readiness forces capable of manoeuvre over strategic distances and equipped with all-domain operating capabilities, predominantly for the competitive phase; the constitution of multi-domain, agile and resilient force structures capable of manoeuvring independently, integrating support through inter-domain fire being manned by professional personnel, selected and trained to operate advanced technologies; the achievement of convergence, which requires the rapid integration of capabilities across all domains, the electromagnetic spectrum and the information environment to maximize effects, approach that leverages inter-domain synergy and employs multiple forms of attack to overwhelm and defeat the adversary. (TRADOC, 2018, pp. 17-20).

The success of implementing these principles relies on the adoption of modern and emerging technologies, the use of highly professional human resources, commanders who are *"capable of making swift decisions and designing dynamic operations"*, and the provision of *"efficient and resilient logistical structures capable*

of promptly delivering the necessary resources and services to combat units, ensuring the support and regeneration of operational efforts" (Minculete, 2023, p. 183).

Russia's threats to the security of the Euro-Atlantic area have spurred the adoption and implementation of the MDO concept in the military doctrine of the North Atlantic Alliance almost simultaneously with the USA, with the transition from joint to multi-domain operations being a strategic priority for NATO. The adoption of the Alliance Concept for Multi-Domain Operations[1] (NATO ACT, 2023, p. 11) marks NATO's shift from a joint approach – centred on the military services coordination – to a multi-domain approach, defined as *"the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance"* (NATO ACT, 2022). Inspired by the considerable US lead, Alliance member nations such as the United Kingdom, Canada, France, Italy, Spain, Germany have focused their efforts on building conceptual frameworks for MDO, conducted exercises, and undertaken initiatives to prepare forces to combat the full spectrum of threats using multi-domain warfare scenarios.

ROMANIAN MILITARY THINKING

The adoption of the Alliance Concept for Multi-Domain Operations marks NATO's shift from a joint approach – centred on the military services coordination – to a multi-domain approach, defined as "the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance".

Guarantees for the implementation of the doctrinal principles of the concept include the establishment of the NATO Response Force (NRF) and the prepositioning of eight multinational battlegroups representing NATO's *"enhanced Forward Presence" (eFP)* on the Alliance's eastern flank, as well as the operationalization of NATO's most recent multinational commands – a corps-level command in Romania and a division-level command in Hungary (Minculete, 2024, pp. 37-39). Additionally, at the NATO summits in Vilnius (2023) and Washington (2024), the need was identified to establish a new *"multinational and multi-domain Allied reaction force, capable of providing a broader range of rapid response options to threats and crises from all directions"* (MAE, 2023). In late 2024, the NRF was replaced by the NATO Allied Reaction Force (ARF), a strategic-level, multi-domain force (NRDC-ITA, 2024). These force structures were initially modelled

[1] The Alliance's MDO Concept was the topic of debates at the NATO MDO Conference in Copenhagen, Denmark, 2023. Session 1 of the Conference states that this document was adopted on 19 May 2023, but, because it is a classified document, it cannot be released to the public, www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Catalogue-April-12.pdf., retrieved on 12 January 2025. (A.N.)

after the Multi-Domain Task Forces (MDTF) established and deployed by the US Army for potential theatres of operations in the Indo-Pacific and Europe (Feickert, 2024).

Countering the threats posed by strategic adversaries in all domains requires, simultaneously with the adoption of doctrinal changes and the reorganization of force structures, the development of integrated multi-domain capabilities that make predominant use of emerging technologies, professional training of forces and commanders, the adaptation of logistical support, and the development of a command-control and communications system that can ensure convergence and synergy of actions and effects across domains.

RUSSIAN PERSPECTIVE ON MULTI-DOMAIN OPERATIONS

The lessons learned from Air-Land Battle principles and derived concepts led to the identification by anti-Western strategic rivals of key conditions that favoured the success of US and NATO military operations and needed to be countered.

The dissolution of the Warsaw Pact followed by the former communist states in Eastern Europe gaining independence and subsequently joining NATO has caused growing concern to the former hegemon to the east. One unacceptable development was the expansion and positioning of the Alliance's military infrastructure ever closer to Russia's borders. Moreover, it led to Russia's loss of a strategic buffer zone between Russia and NATO that enabled it to organize and maintain defence in depth and to ensure freedom of manoeuvre of forces on its territory in the event of an attack. In response, a strategic move by the giant, which had seemed asleep for two decades, was to be expected. Thus, Russian politico-military leaders have closely monitored NATO's and particularly the US's efforts to develop advanced concepts and capabilities, aiming to prepare for a future form of *"high-tech"* warfare. In this evolving battlespace, inter-domain synergies are viewed as a critical factor for achieving success (Griesemer, 2018).

The lessons learned from Air-Land Battle principles and derived concepts led to the identification by anti-Western strategic rivals of key conditions that favoured the success of US and NATO military operations and needed to be countered: gaining access to the theatre of operations and establishing a force projection base through air or sea ports of debarkation; interdependence and interconnectedness among land, sea, air, and even space-based systems; force manoeuvre

capability backed by timely and effective fire support, command-control, and logistical support systems. Subsequently, a process of reorganization of the Russian Armed Forces proved to be urgent, focusing equally on the organization of force structures, modernization of equipment and adaptation of tactics to synchronize operations in several areas. Thus, Russian doctrine has pivoted towards a *"new generation"* warfare that can no longer be equated or confused with non-linear or hybrid warfare, which requires a multi-domain approach.

In its strategic documents, the Russian Federation portrays NATO's actions – such as the expansion of military infrastructure near its borders, intensified information operations, and the increased deployment of larger military force structures and nuclear weapons – as escalating threats to its national security. Moreover, Russia asserts that the United States of America is systematically withdrawing from international arms control agreements while advancing its global missile defence system. Additionally, the deployment of US medium- and short-range missile systems in Europe and the Asia-Pacific region is perceived by Russia as a direct challenge to strategic stability and international security (National Security Strategy of the Russian Federation, 2021, p. 8). As a result, Russia has reiterated the importance of the military domain in achieving its geopolitical objectives of strategic deterrence and conflict prevention. With its return to competition as a global strategic actor, Russia has adopted a strategy aimed at re-establishing a buffer zone between its borders and those of NATO by creating multi-domain layered defence *"bubbles"* using A2/AD capabilities, extending coverage over parts of NATO territory. Despite economic constraints, Russia has focused its efforts on developing advanced A2/AD capabilities consisting of: integrated, multi-layered, long-range air defence systems, incorporating fighter and bomber aircraft, fixed and mobile surface-to-air missile systems, and coastal defence platforms; cruise, ballistic, and intercontinental missiles, capable of being launched from air, sea, and land platforms to strike both land and maritime targets; long-range artillery and precision-guided missile systems, enhancing deep-strike capabilities; next-generation submarines, armed with supersonic anti-ship missiles and ballistic missile systems; kinetic and non-kinetic anti-satellite weapons, supported by dedicated launch infrastructure

With its return to competition as a global strategic actor, Russia has adopted a strategy aimed at re-establishing a buffer zone between its borders and those of NATO by creating multi-domain layered defence "bubbles" using A2/AD capabilities, extending coverage over parts of NATO territory.

and advanced space surveillance systems; advanced cyber warfare and electronic warfare capabilities, designed for information dominance and disruption of adversary networks; search and strike systems based on the use of unmanned vehicles covering air, surface and underwater domains; automated command and control (C2) networks using communications systems protected against adversary interception and countermeasures.

The most threatening and aggressive strategy impacting the security environment on NATO's eastern and southern flanks is Russia's deployment of A2/AD capabilities in Kaliningrad, the Crimean Peninsula, and, to some extent, Syria. This posture is designed to influence, deter, and restrict potential NATO operations in the North Sea, the Baltic Sea, the Black Sea, and the Eastern Mediterranean, as illustrated in *figure 1*.

The most threatening and aggressive strategy impacting the security environment on NATO's eastern and southern flanks is Russia's deployment of A2/AD capabilities in Kaliningrad, the Crimean Peninsula, and, to some extent, Syria. This posture is designed to influence, deter, and restrict potential NATO operations in the North Sea, Baltic Sea, the Black Sea, and the Eastern Mediterranean.

As part of a holistic, multi-domain effort, Russian strategic thinking increasingly emphasizes the importance of informational and psychological actions carried out with military and non-military instruments, integrated and interlinked with traditional military actions to achieve strategic objectives. Russian techniques of disinformation, propaganda and manipulation from the Soviet era have been adapted to the characteristics of the information and security environment of the 21st century, and today have been extended to so-called *computational propaganda*, defined as *"the use of algorithms, automation, artificial intelligence, supported by human intervention, to intentionally distribute misleading information through social networks"* (Howard et al., 2023, pp. 47-53). Their success can be maximized in combination with cyber actions.

The reorganization of force structures and the evolution of operational tactics for modern conflicts have been key components of Russian military doctrine. This transformation reflects a paradigm shift toward an emerging multi-domain force centred around the *battalion-level battle group.* In this new structure, traditional mechanized and armoured combat units are reinforced with capabilities previously reserved for higher echelons, including advanced radar-guided surface-to-air missile systems, long-range artillery and missile systems, unmanned aerial vehicles (UAVs), and electronic warfare assets. This integration enables a single manoeuvre unit

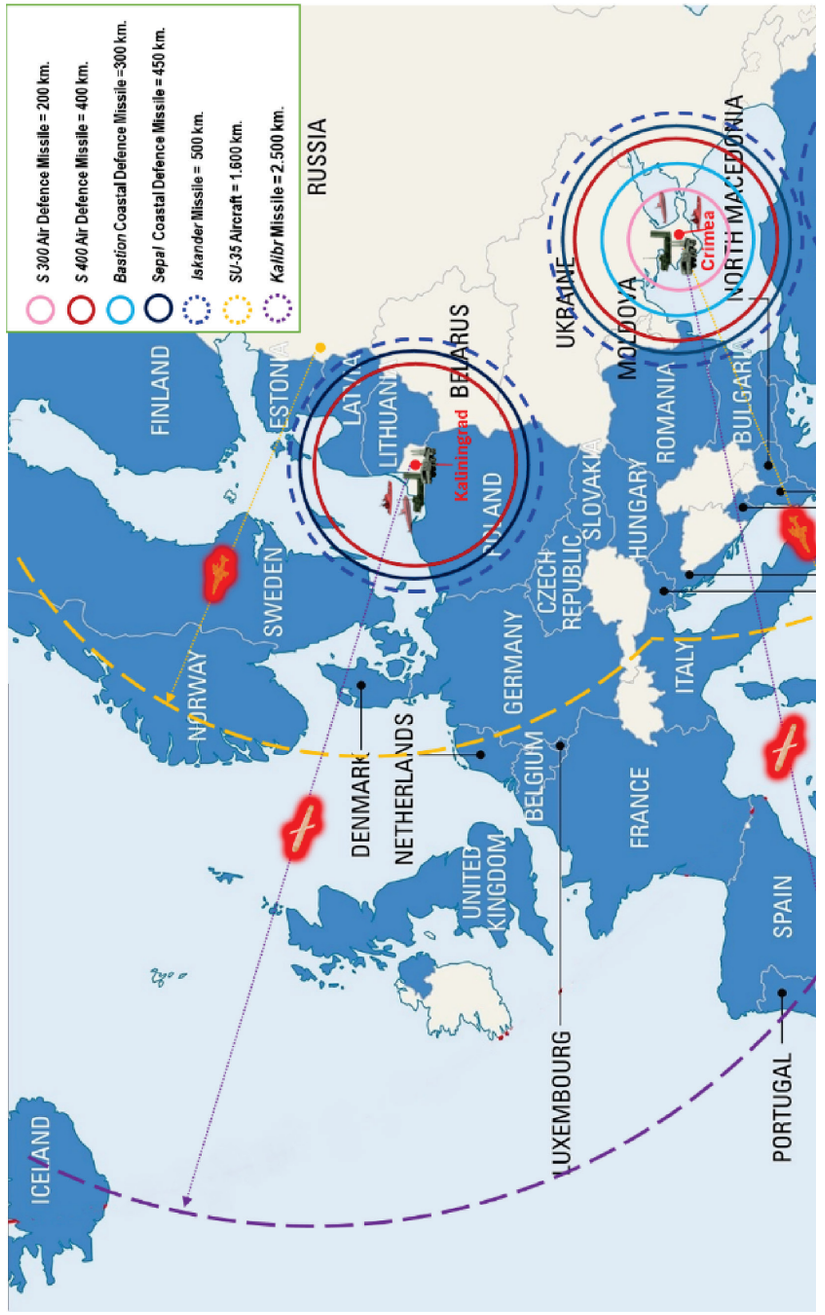

Figure 1: Approximate coverage of Russian A2/AD capabilities on NATO's eastern and southern flank, updated based on Wright and Barrie, 2024

to conduct operations with multi-domain capabilities. The first notable demonstration of this approach occurred on 11 July 2014, during the Zelenopillya attack against Ukrainian mechanized forces. What set this engagement apart was Russia's synchronized use of UAVs, cyber operations, and ground forces under a single battalion commander, achieving a coordinated multi-domain effect. The overwhelming success of this operation not only led to its replication along the Russian-Ukrainian front but also prompted Ukraine and NATO to rapidly develop countermeasures.

An analysis of recent military actions indicates that Russia possesses the capability to conduct complex warfare across multiple domains, with a particular focus on emerging threats and opportunities in the information, cyber, electronic, and space domains. However, Russia's approach to domain integration differs from the Western conceptual framework, as it incorporates several traditional elements of Russian military theory and practice, including:

Russia possesses the capability to conduct complex warfare across multiple domains, with a particular focus on emerging threats and opportunities in the information, cyber, electronic, and space domains.

- *Warfare of the new type* consisting of asymmetric operations conducted in multiple domains, physical and informational, governed by the nuclear threat in order to manipulate the perceptions and decisions of adversaries, shaping their strategic behaviour in directions favourable to Russia;
- *Information warfare* based on the combination and mutual supplementation of information-technical and information-psychological capabilities;
- *Reflexive control* is a strategy designed to achieve mission objectives by deceiving, persuading, coercing, and manipulating an adversary through carefully crafted and targeted information;
- *Disorganization* refers to the deliberate disruption of an adversary's command and control (C2) systems, aiming to degrade their ability to coordinate operations and make effective decisions;
- *Gaining the advantage in the initial period of war* by considering readiness and motivation to fight as determining factors and by taking rapid actions with devastating effects in the initial phases of the conflict that could be decisive in achieving success (Black et al., 2022, pp. 54-57).

Although affected by structural challenges and shortcomings, Russia continues to adapt, seeking to maintain and expand its advantages

in both military and non-military domains. Despite its difficulties, Russian thinking on MDO and related theories is expected to continue to evolve. Russian military thinkers are continually developing new concepts, tactics and methods based on lessons learned from its ongoing operations, spurred by technological developments, as well as as a result of analysing Western approaches with the intention of exploiting the opportunities they present.

CHINA'S PERSPECTIVE ON MULTI-DOMAIN OPERATIONS

The People's Republic of China perceives great power competition as a continuous process of leveraging both military and non-military instruments to achieve its key strategic objectives. This perspective is evident in its implementation of the civil-military fusion strategy and the *"nuclear triad"* doctrine, grounded in the principles of unrestricted warfare. At the same time, China is preparing for potential high-intensity conflicts by emphasizing concepts such as *"information warfare"* and multi-domain *"systems confrontation"*. This approach reflects an unconventional strategy that integrates all available levers of power to gain a competitive edge while remaining below the threshold of armed conflict.

Russian thinking on MDO and related theories is expected to continue to evolve. Russian military thinkers are continually developing new concepts, tactics and methods based on lessons learned from its ongoing operations, spurred by technological developments, as well as a result of analysing Western approaches with the intention of exploiting the opportunities they present.

The reassertion of territorial claims in the South and East China Seas, persistent threats of invasion and annexation of Taiwan, and a lack of transparency regarding the expansion of its military arsenal – including nuclear capabilities – have heightened tensions, intensifying China's rivalry with the USA and its allies at both regional and global levels. Learning the concepts of operation of Western forces, China moved to develop an A2/AD strategy in the Indo-Pacific to protect their interests and deter US power projection in the region, a model later borrowed by Russia. The development of A2/AD capabilities has involved significant investment in new aircraft, sophisticated surface-to-air missiles, modernization of the surface navy and submarine fleet, but the effort has focused on increasing the performance of precision-guided ballistic missiles. American military experts have assessed that, as early as 2019, China possessed *"the most advanced ballistic missile force in the world"* (Impson, 2020), raising doubts about the USA's ability to respond to this threat, overwhelming its missile defence systems. For land-based targets, China has deployed ballistic missiles

that fulfil all three objectives of its A2/AD strategy: DF-31 and DF-41 intercontinental ballistic missiles (ICBMs), with ranges between 11,000 km and 15,000 km, are capable of striking the US mainland; DF-26 medium-range ballistic missile (MRBM), also known as the *"Guam Killer"*, can target US military bases on islands up to 4,000 km away; DF-21D missile, referred to as the *"carrier killer"*, is designed to prevent aircraft carriers from approaching within a range of over 1,700 km (Mihal, 2021). In addition, the development of a network of military bases on artificial islands in the South China Sea has reinforced China's emergence as a global military power, while simultaneously increasing strategic challenges for the USA and its allies in the region. An estimate of the coverage of China's A2/AD capabilities in the Pacific is presented in *figure 2*.

The multi-domain approach in Chinese doctrine is based on proprietary concepts such as "computerized warfare" and "systems confrontation". The former consists in the use of emerging technologies for information acquisition, processing and transmission, the use of artificial intelligence and the robotization of military systems, and the latter is aimed at affecting the nodes and links between elements of an opposing force operating from different domains.

The Chinese military literature increasingly recognizes the strategic relevance of emerging domains such as cyberspace, outer space, electromagnetic and cognitive domains, and considers the information domain to be of primary importance. China's military is increasingly focusing its organization, equipment procurement and training on conducting military operations in information environments that disrupt and dominate adversaries' systems of systems. The multi-domain approach in Chinese doctrine is based on proprietary concepts such as *"computerized warfare"* and *"systems confrontation"*. The former consists in the use of emerging technologies for information acquisition, processing and transmission, the use of artificial intelligence and the robotization of military systems, and the latter is aimed at affecting the nodes and links between elements of an opposing force operating from different domains.

China is excelling in the development and deployment of emerging technologies in the military with capabilities to produce microelectronics, machine components, telecommunications equipment, radars, optical devices, sensors and other products needed to manufacture missiles, drones and tanks. An example is the experimentation in the latest military exercises (Peace Unity-2024 and Golden Dragon-2024) of robot dogs, deployed by drones behind enemy lines and designed to support the military in urban operations with weapon firing, grenade throwing, explosive ordnance disposal capabilities, while being coordinated and supported in the area

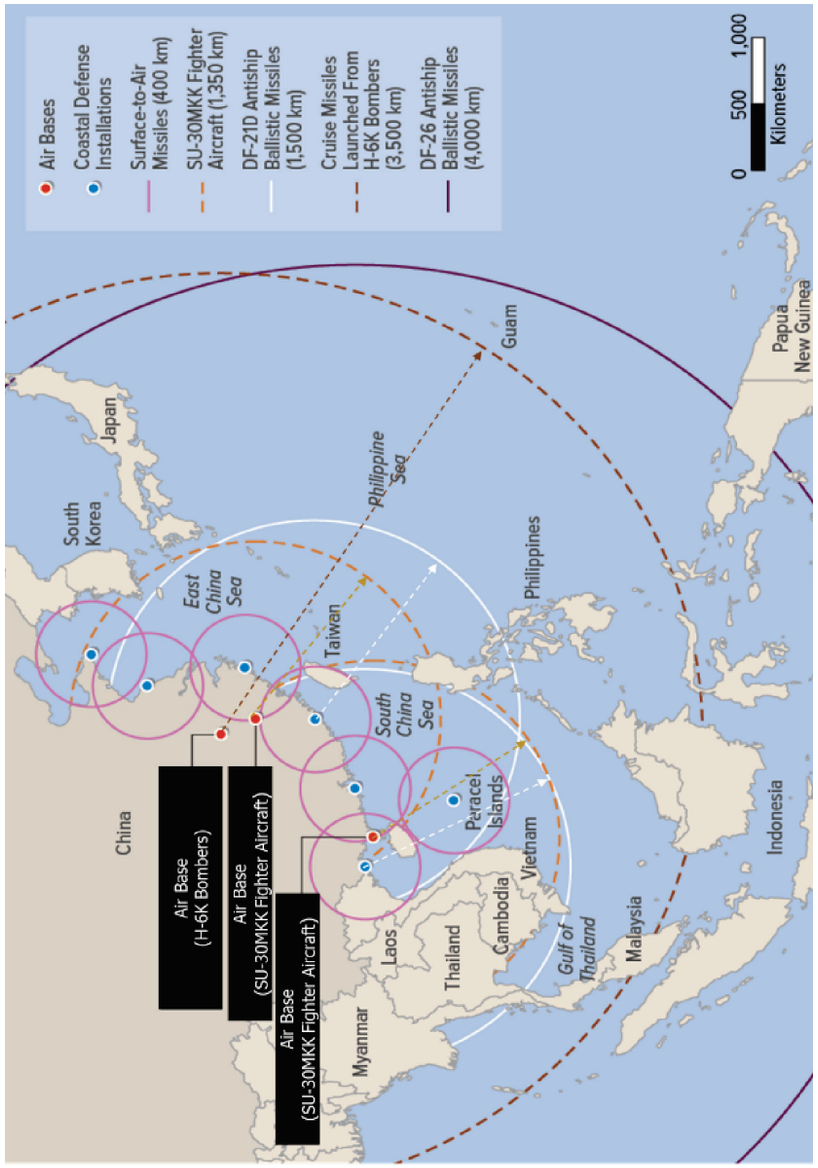

Figure 2: Approximate coverage area of China's A2/AD capabilities in the Pacific (CBO, 2023).

of action by unmanned aerial and ground vehicles (Hurst, 2024, p. 13). The major challenge for Western adversaries lies in China's status as an exporter of these technologies to strategic partners such as Russia, North Korea or Iran, pursuing its economic interests and building sustainable relations with them.

China's latest operational concept called *"Multi-Domain Precision Warfare"* (MDPW) focuses on *"the use of advanced command and control (C2) networks, artificial intelligence, big data analytics, and other modern technologies to identify and exploit critical vulnerabilities in adversaries' operational systems"* (Osborn, 2023). The concept aligns with the military goal to develop a *"mechanized, computerized, and intelligent"* force capable of operating effectively in a warfighting environment characterized by interdependence and multi-domain integration (Withington, 2023). The aim is to coordinate forces from different domains – land, sea, air, space, cyber and electromagnetic spectrum (EMS) – to perform precise strikes against identified vulnerabilities of adversaries. The new type of warfare is based on intelligence, artificial intelligence, connectivity between force services and the ability to achieve new levels of precision in identifying and attacking targets.

China's latest operational concept called "Multi-Domain Precision Warfare" focuses on "the use of advanced command and control (C2) networks, artificial intelligence, big data analytics, and other modern technologies to identify and exploit critical vulnerabilities in adversaries' operational systems".

In the Pentagon's view, the implementation of this concept in Chinese doctrine represents a replication of US development initiatives on the organization of Multi-Domain Task Forces (MDTF) and the development of the Joint All Domain Command and Control Concept (JADC2). This similarity underscores the influence that American concepts of military modernization have on China's emerging strategies, suggesting a continued adaptation of Chinese military forces to keep pace with global trends in multi-domain warfare.

NORTH KOREA'S PERSPECTIVE ON MULTI-DOMAIN OPERATIONS

Over the past decade, North Korea has adopted an approach centred on the development of military concepts and capabilities geared towards an *"asymmetric strategy"* designed to support a type of *"hybrid warfare"* (Black et al., p. 22). This strategy seeks to exploit the critical vulnerabilities of a militarily superior adversary, generating a significant psychological impact that undermines their initiatives,

actions, or will. To achieve these objectives, North Korea maintains a large conventional military force, reinforced by ballistic missiles and nuclear weapons. Additionally, it leverages asymmetric capabilities in emerging operational domains – such as cyber, electronic, and information warfare – to deter aggression. North Korea also employs special operations forces to conduct sabotage, disruption, and neutralization missions targeting adversary command, control, communications, and intelligence (C3I) systems.

Similar to China, North Korea is paying increasing attention to the importance of the information domain, using cyber, electronic warfare and space capabilities to exploit adversaries' vulnerabilities. In the context of actions directed against its main rival, South Korea, there is a subtle shift in strategic priorities from the development of conventional land, air and sea-based military forces to the modernization and diversification of offensive cyber and electronic warfare capabilities. These efforts are geared towards undermining the national will and cohesion of South Korea's alliance with the USA through attacks targeting societal structures, the economy and critical infrastructure.

Despite the difficult economic situation, after 2010, North Korea has prioritized its efforts to increase its military arsenal with a particular focus on ballistic missile development and its nuclear program to deter the United States of America and its allies in the Asia-Pacific region.

Despite the difficult economic situation, after 2010, North Korea has prioritized its efforts to increase its military arsenal with a particular focus on ballistic missile development and its nuclear program to deter the United States of America and its allies in the Asia-Pacific region.

The transformation and modernization of military capabilities has gone through five successive stages, starting with a massive increase in the size of the armed forces, followed by the development of short- and medium-range ballistic missiles (up to 2,500 km), while the nuclear arsenal is being increased as a priority, then the expansion of ballistic missile capabilities to long-range (up to 5,000 km) and intercontinental (over 12,000 km). Pyongyang's ambitions are moving towards supremacy in missile strike, including nuclear missiles, which are considered the most effective means of deterrence, the capabilities of those in service being shown in *figure 3.*

The last two phases have been devoted to modernizing missile strike capabilities for naval forces, stepping up training for special operations forces and, last but not least, equipping the air force with new technologies, including the use of unmanned aircraft (Tasic, 2021, pp. 53-72). North Korea has established specialized military

and civilian units dedicated to electronic, cyber, and information warfare. These efforts are supported by *"surprisingly sophisticated cyber and intelligence capabilities and an institutional base to support these activities"* (Black et al., p. 23).

The integration and coordination of effects across multiple domains can significantly enhance operational effectiveness. The North Korean regime has shown a notable ability to align propaganda and official statements with provocative actions, such as missile tests and nuclear demonstrations, to amplify its strategic and psychological influence.

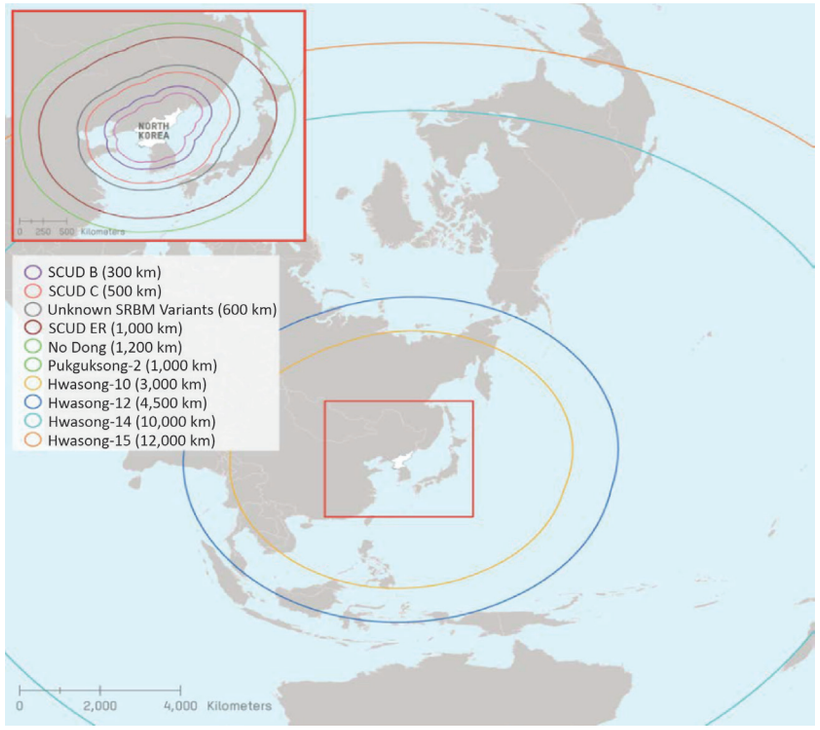

Figure 3: Capabilities of North Korea's ballistic missile systems
(Defense Intelligence Agency, 2021)

The conducted offensive actions, consisting of numerous ballistic missile tests, cyber and electromagnetic spectrum attacks on South Korean military forces and civilian institutions, internal and external propaganda, show that the pursued asymmetric strategy is definitely a non-linear and layered one that has elements in common with the MDO concept but without being backed so far by a capability to integrate and synchronize these cross-domain capabilities. The integration and coordination of effects across multiple domains can significantly enhance operational effectiveness. The North Korean regime has shown a notable ability to align propaganda and official statements with provocative actions, such as missile tests and nuclear

demonstrations, to amplify its strategic and psychological influence. This approach seeks to reinforce perceptions of the seriousness of its threats in order to amplify deterrence.

The regime's lack of transparency and exclusive control over its own media outlets limit access to official information about the North Korean military's operational concepts and doctrine. Therefore, their expansion towards a multi-domain operational framework competing with the West can also be interpreted as a result of intensified military cooperation with Russia and China, but subject to multiple uncertainties.

IRAN'S PERSPECTIVE ON MULTI-DOMAIN OPERATIONS

The rise of US and Western allies' influence in the Middle East at the end of the 20th century posed a major challenge to Iran's interests in maintaining its status as the main power pole in the region.

The rise of US and Western allies' influence in the Middle East at the end of the 20th century posed a major challenge to Iran's interests in maintaining its status as the main power pole in the region. Its geostrategic positioning leads Iran to adopt a 360-degree defence strategy, appreciating that war can start from any direction amid mistrust and historical adversity towards the USA and its close allies. At the same time, North Korea recognizes the necessity of relying on domestically developed military resources, considering the impact of economic sanctions. It has driven the adoption of an asymmetric warfare strategy to offset the imbalance between threats and available resources. Additionally, it has increasingly turned to proxy groups and unconventional warfare methods to extend its influence and counter the US presence across the Middle East.

Iranian concepts of future warfare are based on a general strategy of *"active defence"* and deterrence, using both conventional and asymmetric A2/AD capabilities to resist foreign military incursions, presumed to be US-led (Black et al., pp. 20-21). At the same time, the leadership in Tehran prioritizes securing the regime against internal threats, treating internal stability as a prerequisite for success against external threats. It extends beyond merely suppressing internal dissent, highlighting a strong focus on countering threats from hostile information operations. These threats encompass psychological warfare, espionage, electronic and cyber warfare, as well as precision actions carried out by special operations forces.

Iran's conventional military force consists of the Islamic Republic of Iran Army (Artesh) focused on the defence of national borders. In addition, the state also relies on the Islamic Revolutionary Guards Corps (IRGC), a revolutionary force with additional roles including asymmetric warfare, proxy warfare and internal security, but with control over the ballistic missile program and external operations. The core force services ensure both internal defence and external operations, except for naval and ballistic missile forces, which are dedicated solely to external conflicts. The roles of the IRGC's land and air forces, originally intended for counterinsurgency and territorial defence, can be adapted to support Iran's proxy groups and partners abroad. It is evident in the deployment of counterinsurgency specialists, as well as the use of drones, artillery, and missiles in conflicts across Iraq, Syria, and more recently, the Israel-Palestine conflict. Iran's doctrine utilizes these proxy forces and allied groups, such as Hezbollah and various militias in Iraq and Syria, to project influence and create strategic depth without engaging in direct confrontation.

Iran's deterrence strategy is based on the principle of "Retaliatory Deterrence" or "Threat in Response to Threat", which emphasizes responding to aggression with retaliatory actions severe enough to deter further attacks or prompt rapid de-escalation.

Iran's deterrence strategy is based on the principle of *"Retaliatory Deterrence"* or *"Threat in Response to Threat"*, which emphasizes responding to aggression with retaliatory actions severe enough to deter further attacks or prompt rapid de-escalation (McInnis, 2017, pp. 17-19). In this context, Iran is shifting toward a deterrence approach that leverages emerging technologies and operational domains. To compensate for its limited long-range air power, it continues to develop advanced ballistic and cruise missile systems while significantly expanding its cyber and information warfare capabilities.

Iran's military advances include:

- the development of smart missiles and drones launched from land, helicopter or sea platforms (Dagres, 2024, p. 23);
- the production of medium-range ballistic missiles, most recently the Khorramshahr-4, with a range of 2000 km, while ambitions to produce intercontinental missiles are growing (Rubin, 2024-a, p. 25);
- the space industry's success in launching six satellites to date and building three space launch bases (Rubin, 2024-b, p. 31).

The recent missile attacks from Israel have spurred Iran's military leadership to reassess Iran's air defences and upgrade radars, anti-air

missile systems, electronic warfare systems and drones that will be integrated into the country's air defence cycle as soon as possible.

We assess that Iran is adopting a multi-domain approach by expanding its capabilities across both traditional physical domains and emerging cyber, space, and information domains, leveraging advanced technologies to enhance its strategic reach and effectiveness. A significant challenge in this process is Iran's aim to develop more professional, integrated, and interoperable armed forces. However, this effort is hindered by ongoing competition and redundancy between the Islamic Republic of Iran Army (Artesh) and the Islamic Revolutionary Guard Corps (IRGC), which continues to obstruct improvements in joint and multi-domain operational interoperability.

CONCLUSIONS

Achieving and sustaining strategic superiority in today's security environment necessitates profound transformations and adaptations in military strategy, doctrine, and operational execution for the principal competing powers. A brief analysis of the emergence and evolution of operational concepts shows that they have determined each other in counterbalance and have been adapted according to the strategic interests of each actor, the conditions of economic development, the emergence of new technologies and even the geographical positioning. Thus, we note that the principles of the American Air-Land Battle were countered by A2/AD, asymmetric and hybrid warfare strategies involving action in diverse environments, and later responded to by MDO based on capability integration, convergence and action synchronization. The multi-domain approach, however, presents notable similarities and differences between the main strategic adversaries analysed, which can be summarized as follows:

The principles of the American Air-Land Battle were countered by A2/AD, asymmetric and hybrid warfare strategies involving action in diverse environments, and later responded to by MDO based on capability integration, convergence and action synchronization.

❖ Russia has evolved from a non-linear/hybrid warfare doctrine to a *"new generation"* warfare doctrine, characterized by the synchronization of operations in multiple domains (land, air, sea, space and cyber). It has focused on developing A2/AD capabilities in the Euro-Atlantic region while integrating emerging technologies and multi-domain strategies to counter and deter NATO operations. Russian force structures have been reorganized to reflect an integrated

approach to military operations, with a strong emphasis on multi-domain capabilities such as UAVs, advanced air defence systems, precision missiles, cyber warfare and electronic warfare;

❖ China has enhanced its A2/AD capabilities in the Indo-Pacific region by developing advanced ballistic missiles, sophisticated defence systems, and military infrastructure on artificial islands, aiming to counter and deter US and allied power projection. It has adopted innovative operational concepts such as *"information warfare"* and *"systems confrontation"* aimed at exploiting enemy vulnerabilities;

❖ North Korea has opted for an asymmetric military strategy based on exploiting the vulnerabilities of the superpowers, utilizing unconventional capabilities including cyber and information warfare, ballistic missiles and nuclear weapons. Hybrid warfare and sabotage operations, such as those carried out by North Korean special forces, are essential components of the military strategy, with the aim of causing psychological impacts and destabilizing the strategic infrastructures of adversaries;

❖ Iran is investing heavily in the development and deployment of A2/AD capabilities, such as ballistic missiles, advanced air defence systems and attack drones. It applies a concept of hybrid warfare, combining cyber, intelligence and asymmetric operations capabilities to influence public opinion and destabilize NATO or US alliances in the region. Iran has a vast network of *proxy* groups and allies that can be used to wage asymmetric warfare on multiple fronts, complicating any multi-domain strategy.

While Russia, China, Iran, and North Korea do not explicitly adopt a "multi-domain" doctrine, their military strategies exhibit multi-domain characteristics similar to those found in the USA and NATO doctrine. It can be inferred from their force structure reorganizations, capability development priorities, and the tactics employed in recent military operations and exercises.

Therefore, while Russia, China, Iran, and North Korea do not explicitly adopt a *"multi-domain"* doctrine, their military strategies exhibit multi-domain characteristics similar to those found in the USA and NATO doctrine. It can be inferred from their force structure reorganizations, capability development priorities, and the tactics employed in recent military operations and exercises.

In the face of rapid and aggressive response adaptations by major strategic competitors, we identify several implications for strengthening the future approach to US- and NATO-led multi-domain operations:

- continued investments to integrate advanced technologies into equipment (artificial intelligence, augmented reality, cyber weapons, and autonomous systems) that support the integration and synchronization of MDO;
- ensuring excellent interoperability between NATO forces, particularly for command and control (C2) systems;
- building robust cyber resilience, improving information defence and countering disinformation capabilities;
- expanding cooperation with regional and global allies, as well as strengthening partnerships with third states and international organizations;
- testing and validating doctrines for MDO through integrated military exercises;
- training and equipping military personnel to conduct MDO.

These implications highlight the necessity of developing an integrated, flexible, and innovative approach to address future strategic challenges, particularly in response to the emerging capabilities of adversaries and the growing complexity of *"multi-domain warfare"* on a global scale.

BIBLIOGRAPHY:

1. Black, J. et al. (2022). *Multi-Domain Integration in Defence Conceptual Approaches and Lessons from Russia, China, Iran and North Korea*. RAND Corporation.
2. CBO (2023). *U.S. Hypersonic Weapons and Alternatives,* Congressional Budget Office, https://www.cbo.gov/publication/58924, retrieved on 21 October 2024.
3. Dagres, H. (2024). *Iranian Military Equipment Integrating Artificial Intelligence*. Operational Environment Watch (8), p. 23, https://fmso.tradoc.army.mil/oe-watch-previous-issues/, retrieved on 11 March 2024.
4. Defense Intelligence Agency (2021). *North Korea – A Growing Regional and Global Threat*, p. 27, https://www.dia.mil/Military-Power-Publications/, retrieved on 10 April 2024.
5. Dwight, P. (2023). *Multi-Domain Operations: Passing the Torch.* Hague: The Hague Centre for Strategic Studies, https://hcss.nl/report/multi-domain-operations-passing-the-torch/, retrieved on 17 May 2024.
6. Feickert, A. *The Army's Multi-Domain Task Force (MDTF),* Congressional Research Service, https://sgp.fas.org/crs/natsec/IF11797.pdf, retrieved on 19 April 2024.
7. Griesemer, T. (2018). *Russian Military Reorganization: A Step Towards Multi-Domain Operations*. OTH: Multi-Domain Operations&Strategy,

https://othjournal.com/2018/11/19/russian-military-reorganization-a-step-toward-multidomain-operations/, retrieved on 29 May 2024.
8. Howard, P. et al. (2023). *Computational propaganda: Concepts, methods, and challenges.* Sage Journal, 8(2), pp. 47-53, https://doi.org/10.1177/20570473231185996, retrieved on 19 September 2024.
9. Hurst, C. (2024). *China Introduces New Unmanned Systems in Combat Exercises.* Operational Environment Watch (8), 13, https://fmso.tradoc.army.mil/oe-watch-previous-issues/, retrieved on 12 December 2024.
10. Impson, N. (2020). *The Next Warm War: How History's Anti-Access/Area Denial Campaigns Inform the Future of War.* In *Small Wars Journal*, https://archive.smallwarsjournal.com/comment/62423, retrieved on 15 November 2024.
11. Lund-Hansen, K., Reilly, J. (1 November 2024). The Multi-Domain Operations Approach to Intermediate PME, WAR ROOM: https://warroom.armywarcollege.edu/articles/competencies-6/, retrieved on 5 February 2025.
12. Ministerul Afacerilor Externe/MAE/Ministry of Foreign Affairs (11 July 2023). *Comunicatul Summitului NATO de la Vilnius/NATO Vilnius* Summit Communiqué, mae.ro, https://www.mae.ro/node/62432, retrieved on 22 December 2024.
13. MAE (2024). *Declarația Summitului de la Washington emisă de șefii de stat și de guvern care au participat la reuniunea Consiliului Nord-Atlantic din Washington, D.C./NATO Washington Declaration*, https://www.presidency.ro/ro/media/comunicate-de-presa/washington-summit-declaration-issued-by-the-heads-of-state-and-government-participating-in-the-meeting-of-the-north-atlantic-council-in-washington-d-c-10-july-2024, retrieved on 21 October 2024.
14. McInnis, M. (2017). *Iranian Concepts of Warfare – Understanding Tehran's Evolving Military Doctrines*. American Enterprise Institute, pp. 18-19, retrieved on 25 September 2024.
15. Mihal, C.J. (July-August 2021). *Understanding the People's Liberation Army Rocket Force Strategy, Armament, and Disposition.* In *Military Review*, pp. 220-234, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/China-Reader-Special-Edition-September-2021/Mihal-PLA-Rocket-Force/, retrieved on 25 November 2024.
16. Minculete, Gh. (2023). *Abordări conceptuale, organizatorice și relaționale privind operațiile multi-domeniu*. In *Gândirea militară românească*, pp. 164-185.
17. Minculete, Gh. (2024). *Augmentarea logisticii operațiilor joint multinaționale în condiții de modernitate și progres.* Sibiu: Academia Forțelor Terestre *"Nicolae Bălcescu".*
18. NATO ACT (2022). *Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries,* Allied Command Transformation,

https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/, retrieved on 5 November 2024.
19. NATO ACT (10-11 October 2023). NATO Multi-Domain Operation Conference 2023. Report, www.act.nato.int: www.act.nato.int/wp-content/uploads/2024/05/2024-MDO-Catalogue-April-12.pdf., retrieved on 27 November 2024.
20. NRDC-ITA (2024). *NATO Allied Reaction Force*, nrdc-ita.nato.int: https://nrdc-ita.nato.int/operations/allied-reaction-force, retrieved on 22 November 2024.
21. Osborn, K. (2023). *China's New "Multi-Domain Precision Warfare" Operational Concept "Mirrors" US Strategy*, https://warriormaven.com/china/chinas-new-multi-domain-precision-warfare-operational-concept-completely-mirrors-us-strategy, retrieved on 2 February 2025.
22. Rubin, M. (2024-a). *Iran Highlights Recent Missile Achievements. Operational Environment Watch*, p. 25, https://fmso.tradoc.army.mil/oe-watch-previous-issues/, retrieved on 11 April 2024.
23. Rubin, M. (2024-b). *Iran Spaceport to Open in 2025*. *Operational Environment Watch*, p. 31, https://fmso.tradoc.army.mil/oe-watch-previous-issues/, retrieved on 11 April 2024.
24. *National Security Strategy of the Russian Federation* (2021), https://rusmilsec.blog/wp-content/uploads/2021/08/nss_rf_2021_eng_.pdf, retrieved on 17 November 2024.
25. Tasic, M. (2021). *Exploring North Korea's Asymmetric Military Strategy.* In *Naval War College Review*, 72(4), pp. 53-72, https://www.jstor.org/stable/26775519, retrieved on 10 December 2024.
26. TRADOC (2018). *Pamphlet 525-3-8, U.S. Army Concept for Multi-Domain Combined Arms Operations at Echelons above Brigade.* Virginia, SUA: U.S. Army Training and Doctrine Command.
27. U.S. Army. (2022). *FM 3-0 Operations*, Headquarters Department of the Army, Washington, D.C.
28. U.S. DoD (2022). *U.S. National Defense Strategy, Department of Defense,* https://www.defense.gov/National-Defense-Strategy, retrieved on 14 September 2024.
29. Withington, T. (2023). *MDO with Chinese Characteristics,* Armada International, https://www.armadainternational.com/2023/11/chinese-military-communications-modernisation/, retrieved on 10 October 2024.
30. Wright, T., Barrie, D. (2024). *The return of long-range US missiles to Europe*, https://www.iiss.org/online-analysis/online-analysis/2024/08/the-return-of-long-range-us-missiles-to-europe/, retrieved on 14 October 2024.