IMPLICATIONS OF HYBRID WARFARE ACTIVITIES ON THE MULTI-DOMAIN OPERATIONS OF NAVAL FORCES IN THE BLACK SEA

Navy Captain (Ret.) Professor Ion CHIORCEA

"Mircea cel Bătrân" Naval Academy, Constanța

Lieutenant Commander Andrei PAVĂL, Doctoral Student

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2025.3.18

In a context marked by the strategic competition between the North Atlantic Treaty Organization and the United States of America, on the one hand, and the Russian Federation, on the other hand, the analysis begins with the definition of doctrinally recognized operational domains: land, air, maritime, space, and cyber, to which are added the cognitive/information dimension and the civil cooperation dimension. The applied methodology relies on a multi-criteria comparative analysis of the implications of hybrid warfare activities on each domain, by identifying five relevant types of threats. The expected results are aimed at providing a doctrinal basis for establishing multi-domain formations within NATO and their applicability at the national level, with an emphasis on the specific features of the Black Sea operational environment. The novelty element lies in the systematic correlation of hybrid warfare threats with the integration capacity of multi-domain formations, offering recommendations for adapting naval forces towards the 2030 horizon.

Keywords: hybrid warfare; multi-domain operations; naval forces; Black Sea; multi-domain formations;

INTRODUCTION

The current international security environment is characterized by heightened strategic competition, in which great powers vie for supremacy across all dimensions of the operational environment. Recent conflicts, from the Russian Federation's aggression against Ukraine to escalations in the Middle East, have demonstrated that the boundaries between peace, crisis, and war are increasingly blurred, and military operations can no longer be conceived solely through the lens of a single operational domain. In this context, the concept of multi-domain operations (MDO) has emerged as a doctrinal response to the complexity of the strategic environment, being institutionalized by the US Armed Forces and gradually adopted by the North Atlantic Treaty Organization (NATO) as a foundation for future campaign planning.

At the US level, initiatives such as JADC2 (Joint All-Domain Command and Control) and *"project overmatch"* constitute the pillars of military transformation. JADC2 aims to create an integrated architecture capable of connecting sensors and effectors across all domains into a single network, in order to deliver rapid decision-making in an environment saturated with electromagnetic warfare and cyberattacks. In parallel, the US Navy seeks, through *"project overmatch"*, to integrate artificial intelligence and autonomous systems into dispersed naval operations, in order to maintain the advantage in an increasingly contested maritime domain (Hoehn, 2021). Both programs confirm the strategic direction toward the year 2030[1] (Cucinschi, 2024), a direction doctrinally reinforced through *"FM 3-0 Operations"* (2025), which explicitly states that *"all operations are multi-domain operations"* (Headquarters, Department of the Army, 2025, p. 17), applicable at all echelons and in all strategic contexts: peace, crisis, and war (Ib., pp. 16-17).

[1] The United States' objective was defined in *"TRADOC Pamphlet 525-3-1"* (2018), which refers to an army capable of multi-domain operations (MDO) by the year 2028 (US Army Training and Doctrine Command, 2018). Subsequently, *"FM 3-0 Operations"* (2022) explicitly referred to the 2030 timeframe under the *"Army 2030"* vision, while the updated edition, *"FM 3-0 Operations"* (2025), no longer sets a calendar year but doctrinally reinforces the principle that "*all operations are multi-domain operations"* (Headquarters, Department of the Army, 2025). Within NATO doctrine, the concept of MDO was officially institutionalized through *"AJP-3 Allied Joint Doctrine for the Conduct of Operations"* (2019) and later expanded by Allied Command Transformation (2025), though without specifying a precise year for implementation. In this study, the year 2030 is employed as an analytical benchmark, inferred from the US objective and the presumed alignment of the Alliance as a whole with this strategic direction.

In parallel, NATO explicitly acknowledged the importance of multi-domain integration through *“AJP-3, Allied Joint Doctrine for the Conduct of Operations”* (2019), as well as within specialized conferences held under Allied Command Transformation (Allied Command Transformation, 2025). They institutionalize not only the classical domains: land, air, maritime, space, and cyber, but also emphasize the significance of the cognitive/information dimension and the civil cooperation dimension as indispensable functions for achieving operational superiority (North Atlantic Treaty Organization, 2019). Thus, the Allied framework confirms that the success of multi-domain operations depends on integrating military and civilian resources, shaping perceptions, and strengthening social resilience.

Nevertheless, the application of MDO in geographically constrained and contested regions such as the Black Sea raises significant challenges. The Pontic area is marked by the presence of the Russian Federation Navy (RFN), the militarization of the Crimean Peninsula, and the use of hybrid techniques and tactics (e.g., disinformation, cyberattacks, exploitation of civilian infrastructure, challenging the international legal regime etc.). At the same time, for NATO and the littoral states, the Black Sea holds a distinct strategic role by ensuring freedom of navigation, securing maritime energy infrastructure, and supporting vulnerable partners (Vdovychenko, Albu, Chitadze, 2024; Kohler, 2020). This dual relevance, vital for both Russia and NATO, creates the premises of a contested environment, where hybrid warfare activities become instruments for eroding cohesion and undermining freedom of navigation in the Black Sea.

Previous research has focused primarily on the doctrinal definition of MDO and on the development of technological capabilities required for its implementation. However, it remains unclear to what extent hybrid warfare activities can undermine multi-domain convergence in semi-enclosed theatres of operations such as the Black Sea. This gap is particularly relevant for Romania, a Black Sea littoral state which, through its NATO membership, follows the trajectory of implementing multi-domain formations (MDF) by the 2030 horizon. Nevertheless, structural vulnerabilities, such as insufficiently protected critical port infrastructure, dependence on civilian resources, and lack of strategic depth, raise questions regarding the pace and consistency of practically translating this objective into reality.

The purpose of this study is to critically examine the implications of hybrid warfare activities on each domain of MDO, with particular focus on the Black Sea operational environment and on the role of the Romanian Naval Forces.

The proposed methodology, a multi-criteria comparative analysis, enables the identification of five types of hybrid warfare threats for each domain/dimension and the assessment of their implications for the practical implementation of MDO through MDF. The results aim both to clarify vulnerabilities and to formulate doctrinally and operationally applicable recommendations designed to enhance the resilience of the naval forces and their interoperability with the Allies.

The novelty of this study originates from the systematic correlation of hybrid activities with the vulnerabilities of MDO domains and their translation into a forward-looking framework for the implementation of naval MDF in the Black Sea. This approach does not remain confined to a theoretical description but seeks to provide a comparative, future-oriented framework for Allied strategic planning in the Black Sea region. In this way, the study contributes to the specialized literature and delivers practical value for the Romanian Naval Forces, demonstrating that the success of implementing MDF towards 2030 depends not only on technological modernization and doctrinal adaptation but also on the ability to effectively counter hybrid warfare activities that define the current security environment.

This analysis is based on the hypothesis that hybrid activities generate asymmetric effects across different domains, being particularly pronounced in the maritime domain while maintaining close interdependence with the other operational domains. The central research question guiding this study is: *How do hybrid warfare activities affect the capacity of the naval forces in the Black Sea to implement MDO by the 2030 horizon, and what doctrinal, technological, and organizational adaptations are required for multi-domain formations?* To answer this question, the research seeks to define the domains of MDO and tailor them to the specifics of the Black Sea region, to identify and analyse five relevant hybrid warfare activities for each domain, to assess their implications through a multi-criteria comparative analysis, and to examine their impact on the Romanian Naval Forces and NATO. Finally, the study proposes doctrinally and operationally applicable recommendations intended to strengthen resilience and interoperability within MDF. The structure of the paper follows a logical progression, from the conceptual analysis of MDO domains and the identification of relevant hybrid warfare threats, to the application of a multi-criteria comparative method and the extraction of conclusions and recommendations for the doctrinal and operational adaptation of the naval forces.

STATE OF THE ART IN THE FIELD

The specialized literature on hybrid warfare is extensive, reflecting the constant concern of both the academic and doctrinal communities with the ambiguous and multidimensional nature of this type of conflict. Analyses emphasize that hybrid warfare entails a fluid combination of conventional and unconventional means, both military and non-military, to exploit the vulnerabilities of adversaries. Ferris (2012) shows that the phenomenon is not new, having historical roots in imperial conflicts, but has gained increased relevance in the 21st century. Batyuk (2017) highlights that the term was adopted by the United States of America as a conceptual tool to describe tactics of strategic coercion below the threshold of conventional conflict. Grier (2017) warns of the risk that *"hybridity"* may become a mere *buzzword*2, losing analytical value, an idea echoed by Wither (2023), who criticizes the lack of conceptual clarity. In the same vein, Tagarev (2021) proposes new analytical frameworks for hybrid warfare threats, stressing the need for a systemic approach.

In the maritime domain, recent research confirms the adaptability of hybrid warfare and, implicitly, the activities associated with this type of conflict. Studies such as those by Schaub, Murphy and Hoffman (2017) or Mitrescu and Sokolov (2025) show that critical maritime infrastructure has become a primary target for hybrid warfare threats, while Stensrud and Østhagen (2024) describe the tactical application of Russian new-generation warfare in areas such as the Arctic and the Black Sea. These works confirm that hybrid warfare plays a central role in strategies of destabilization and in challenging the international order.

With regard to MDO, the literature remains at an early stage, being strongly influenced by US doctrine. The manuals – US Army Training and Doctrine Command (2018) and Headquarters, Department of the Army (2025) have established MDO as a new operational concept, defining the simultaneous integration of all domains to create relative advantages over adversaries. Complementarily, reports on JADC2 and *"project overmatch"* (Hoehn, 2021) indicate the technological direction of integrating sensors and effectors across all domains. At the NATO level, doctrine (North Atlantic Treaty Organization, 2019) and recent initiatives of Allied Command Transformation (2025) confirm the relevance of the multi-domain operations approach, though without specifying a clear implementation timeline. According to US doctrine, it is necessary to distinguish between MDO, defined as a doctrine that integrates all domains to create relative advantages, and MDF, conceived

[2] The term *"buzzword"* refers to a fashionable word or expression, frequently used in political, academic, or media discourse, risking the loss of its analytical meaning through overuse and ambiguity.

as organizational instruments through which this doctrine is put into practice, designed to penetrate and disintegrate adversary A2/AD (Anti-Access/Area Denial) systems and exploit the advantage and freedom of manoeuvre thus achieved (US Army Training and Doctrine Command, 2018, p. 5). Nevertheless, although MDF are theoretically presented as ideal solutions for the operationalization of MDO, their application in restricted, semi-enclosed, and contested maritime spaces such as the Black Sea raises questions regarding the feasibility and adaptability of this model to regional geopolitical and infrastructural realities.

Last but not least, at the academic level, Kohler (2020) highlights the necessity of integrating naval forces into the Joint Force Maritime Component Command in order to counter Russian influence in the Black Sea, while Vdovychenko, Albu and Chitadze (2024) analyse the region's security trilemma, defined by the interaction between Türkiye's own interests, the pro-western orientation of Ukraine and the allied Black Sea littoral states, and the Russian Federation's objective of maintaining its influence. Other contributions, such as Islam (2024) and Scutaru, Pavel (2025), expand the debate on regional cooperation and on the resilience of critical infrastructure.

A critical review of the specialized literature reveals a disproportion: the amount of work on hybrid warfare is abundant and diverse, with numerous case studies and conceptual approaches, while research on MDO, particularly with respect to the Black Sea region, remains anchored mainly in US doctrine and NATO's early attempts at adaptation. Moreover, causal analysis of how hybrid warfare activities directly influence the implementation of MDO is nearly absent. This gap justifies the present study, which proposes a systematic correlation between the two concepts and their contextualization for the Black Sea theatre of operations. In this regard, the need to examine hybrid warfare threats in the Pontic area, intensively studied and debated in the literature, becomes essential for understanding how they affect the applicability of MDO and, implicitly, MDF in the region. Furthermore, given that state actors such as the United States of America are approaching the final phase of the timeline assumed for the implementation of these MDF, shaping the operational environment prior to implementation is imperative in order to support both doctrinal adaptation and the practical preparation of the Romanian Naval Forces and NATO in the Black Sea.

METHODOLOGY

The methodology of this article is designed to provide a systematic analytical framework through which the central objective can be achieved: identifying the implications of hybrid warfare activities on MDO and on the capacity of the naval forces in the Black Sea to implement multi-domain formations by the 2030 horizon. This methodological approach is directly aligned with the research question and the previously stated objectives, offering the instruments through which the analysis can highlight how these implications influence the practical translation of MDO and MDF doctrines in the Black Sea region. In military research, methodology is not merely a set of technical procedures but represents the foundation through which data are collected, interpreted, and transformed into doctrinally applicable results (Creswell, Creswell, 2018).

The main method employed is a multi-criteria comparative analysis of the implications of hybrid warfare activities on each domain/dimension of MDO. The selection of this method is justified by the complex and interdependent nature of operational domains, where threats cannot be analysed in isolation but only in relation to an integrated whole. The model is inspired by multi-criteria assessments applied in security studies, which enable the qualitative quantification of implications (Tagarev, 2021). Within this framework, the research identifies five hybrid warfare activities representative for each MDO domain, selected on the basis of specialized literature and NATO and US doctrinal documents, though not limited exclusively to these sources.

The data used derive from doctrinal documents, which provide the conceptual framework and the implementation timeline; from recent academic literature, which offers critical perspectives on hybrid warfare and MDO, as well as from regional case studies specific to the Black Sea, focused on the effects of hybrid tactics on maritime security. The processing of these data involves scoring the identified hybrid warfare activities, assessing their implications (intensity, probability, and relevance) on a scale from 1 to 5, and integrating them into a comparative matrix.

The selection of the 1-to-5 scale has a methodological foundation. According to Creswell and Creswell (2018), the use of a simple and standardized scale allows the integration of qualitative and quantitative data into a convergent mixed-methods approach. In this article, the value 1 corresponds to minor implications, where the hybrid activity has limited effects on the analysed domain, while the value 5 designates critical implications, capable of decisively affecting cohesion and multi-domain integration capacity. Intermediate values (2-4) reflect gradations of intensity, probability, and relevance, calibrated on the basis of frequency and severity (impact) identified in the specialized literature and doctrinal documents. This scaling facilitates comparability across domains and transforms qualitative analysis into a predictive tool with applicability for operational planning (Creswell, Creswell).

The analysis is critically oriented, in the sense that it does not limit itself to reproducing doctrinal definitions but seeks to highlight the discrepancies between theory and practical applicability. For example, US Army Training and Doctrine Command (2018) clearly defines the distinction between MDO as doctrine and MDF as an organizational instrument, yet it remains unclear how these MDF can be adapted to semi-enclosed and contested spaces such as the Black Sea. For this reason, the research proposes correlating the implications of hybrid warfare activities with the vulnerabilities of each MDO domain, as an exercise in anticipatory modelling prior to the actual implementation of MDF.

Through this approach, the methodology contributes not only to validating the research question but also to establishing an analytical framework that can be replicated in other similar maritime regions. In addition, the results obtained will support the doctrinal adaptation of the Romanian Naval Forces and may provide a planning instrument oriented toward resilience and interoperability. The structure of the following chapters reflects this approach: first, the MDO domains will be defined with a particular focus on the Black Sea region. Then, each domain will be analysed in relation to the implications of hybrid warfare activities, based on the previously described method.

DOMAINS AND DIMENSIONS OF MULTI-DOMAIN OPERATIONS AND THEIR PARTICULARIZATION FOR THE BLACK SEA REGION

MDO represent one of the most significant doctrinal transformations of the 21st century, providing an integrated framework through which armed forces can achieve simultaneous superiority across all dimensions of modern conflict. Studying the dimensions of MDO is essential not only for understanding the mechanisms through which great powers project force, but also for identifying vulnerabilities that adversaries may exploit through hybrid warfare activities. States such as the USA have adopted the concept of multi-domain operations (MDO) as a reference doctrine and have initiated the development of multi-domain task forces (MDTF) as experimental structures, designed to penetrate and disintegrate A2/AD systems and to exploit the advantage and freedom of manoeuvre thus achieved.

They represent the precursors of multi-domain formations (MDF) currently under development, intended to ensure in the future the large-scale implementation of MDO and to consolidate an anticipatory approach to strategic competition (US Army Training and Doctrine Command, 2018). For the Black Sea context, the present analysis will refer exclusively to the concept of MDO and to MDF, given that MDTF remain experimental structures, developed at present only by the United States of America. In this context, the analysis of MDO begins with the definition of doctrinally recognized operational domains: land, air, maritime, space, and cyber, to which are added the cognitive/information dimension and the civil cooperation dimension. In contested and semi-enclosed regions such as the Black Sea, contextualizing the domains and dimensions of MDO becomes a critical condition for operationalizing the doctrine and for adapting the naval forces to NATO requirements and the characteristics of the current security environment.

Land Domain

It constitutes the fundamental dimension of warfare, as it encompasses control of physical space, force mobility, and support for operations in the other domains. Current US doctrine emphasizes that land manoeuvre does not occur in isolation but is permanently interconnected with effects generated in the air, maritime, space, and cyber domains (Headquarters, Department of the Army, 2025). This approach reflects the transformation of land operations from a traditional dimension into a vector of multi-domain integration.

Within MDO and MDF, the land domain acquires particular relevance through its role in penetrating and disintegrating A2/AD systems, thereby facilitating freedom of action for air, naval, and space forces (US Army Training and Doctrine Command, 2018). Thus, land forces no longer have an exclusively ground manoeuvre role but become an integral part of a system that generates simultaneous relative advantages across all domains.

Across the Black Sea region, the land domain has critical particularities: the territories of Romania and Bulgaria serve as strategic staging points for NATO force deployment, while road, rail, and force logistics infrastructure constitute an essential condition for supporting air and maritime operations. However, this infrastructure can become vulnerable to hybrid sabotage of transport routes and logistic facilities (Eckel, 2025), to the infiltration of proxy and paramilitary forces supported externally (Beznosiuk, 2025), or to lawfare3 tactics that challenge troop deployments and generate strategic ambiguity (Bachmann, Mosquera, 2015). In parallel, the use of suicide drones and loitering munitions4 transforms the tactical battlefield into an environment saturated with asymmetric risks (Kunertova, 2023), while GNSS (Global Navigation Satellite System) jamming and spoofing5 can undermine the coordination and mobility of land forces (Schmidt, Radke, Camtepe, Foo, Ren, 2016). In addition, capabilities such as amphibious assault and special operations forces directly connect the land domain with the maritime and air domains, providing flexibility in countering these hybrid warfare activities and in supporting integrated multi-domain operations.

Air Domain

It represents one of the essential domains of power projection, providing rapid mobility, strategic surveillance, and precision strike capability. US doctrine defines airpower as an indispensable instrument for achieving superiority in modern conflict, emphasizing its interdependence with the other operational domains (US Air Force, 2021). By virtue of its flexible and global character, airpower enables decisive actions within short timeframes; however, it faces significant constraints in highly contested operational environments such as the Black Sea, dominated by A2/AD systems.

In the context of MDO, the air domain plays a central role in integrating reconnaissance, command, and strike systems, while simultaneously supporting land, naval, and space forces. MDF depend on aviation for penetrating A2/AD systems and for synchronizing effects across all domains (US Army Training and Doctrine Command, 2018). Thus, aviation is not merely a supporting vector but a critical link for the success of multi-domain operations.

In the Black Sea region, the air domain faces complex particularities: the presence of Russian S-400 air defence systems in Crimea restricts freedom of air manoeuvre, while GNSS jamming undermines navigation and coordination.

[3] The term *lawfare* comes from the combination of law and warfare and involves the strategic use of legal instruments as a weapon of war, with the aim of limiting the opponent's freedom of action, challenging the legitimacy of troop deployment or creating strategic ambiguities. The concept is analysed in the international security literature as part of the spectrum of actions associated with hybrid warfare, being correlated with both the manipulation of the international legal framework and the exploitation of domestic regulations to achieve political-military objectives (Orde, 2016).

[4] The term *loitering munition* designates a type of unmanned aerial weapon that combines the characteristics of a drone with those of a precision munition.

[5] The term *spoofing* designates a computer attack technique through which false signals or data are generated, intended to imitate legitimate sources, with the aim of deceiving receiving systems.

The use of drones and loitering munitions has demonstrated the vulnerability of air bases and critical infrastructure (Kunertova, 2023; Plichta, 2025). In addition, electromagnetic warfare operations, cyberattacks against aviation infrastructure, and multi-vector saturation strikes put the resilience of air forces under pressure, creating significant risks for the air domain as part of MDO in the Black Sea region (Florido-Benítez, 2024; Dalsjö, Jonsson, Norberg, 2022).

Maritime Domain

Alongside the air domain, it is another vital domain for power projection and freedom of navigation, ensuring both control of sea lines of communication (SLOC) and protection of critical infrastructure. US naval doctrine emphasizes that maritime power integrates surface, submarine, and air-maritime actions, being indispensable for deterring adversaries and for ensuring access to contested areas (US Navy, 2025). From a multi-domain perspective, naval capabilities provide strategic mobility and support for land and air operations, while simultaneously depending on informational and cyber integration.

As part of MDO, the maritime domain plays a central role in penetrating A2/AD systems and in maintaining the freedom of manoeuvre of Allied forces. The role of MDF can be to generate simultaneous effects on the surface, underwater, and in the air domain, thereby supporting synchronization with land and air forces (US Army Training and Doctrine Command, 2018). Thus, the navy is not merely a force of presence and deterrence but a critical component of multi-domain integration.

Throughout the Black Sea area, the maritime domain is strongly influenced by the presence and militarization of the RFN, as well as by the location of critical infrastructure in close proximity to risk areas. Specific hybrid warfare activities include the sabotage of critical maritime infrastructure, the use of autonomous naval drones against ports and ships, AIS/GPS (Automatic Identification System/Global Positioning System) navigation system spoofing, the disruption of commercial traffic through the declaration of maritime areas as exercise zones, and the deliberate harassment of vessels through dangerous approach manoeuvres (Monaghan, Connolly, 2023, p. 23; Burlacu, Sandu, 2023; Zorri, Kessler, 2024; Gaber, 2024; Sabanadze, Dalay, 2025; Godzimirski, Mitrescu, 2025). These tactics increase the risk of escalation and undermine regional maritime security, affecting the capacity of the maritime domain to be integrated into multi-domain operations.

Space Domain

It has become a central pillar of modern operations, providing secure communications, global surveillance, and support for navigation and the precise guidance of modern munitions. US Space Force (2025) defines space as a distinct operational environment, in which the control and protection of satellite infrastructure are essential for the conduct of any military campaign. In the current logic of warfare, satellites no longer serve solely as tools for information gathering but have become direct operational instruments within the multi-domain architecture.

Embedded in MDO, the space domain is critical for simultaneously connecting all domains, from land and maritime to air and cyber. MDF rely on satellite services for action coordination and for ensuring the resilience of command and control (C2) systems in highly contested operational environments (US Army Training and Doctrine Command, ib.). Space, by its global nature, provides freedom of manoeuvre and informational superiority but at the same time becomes a hybrid confrontation arena where strategic competition is intense.

Across the Black Sea region, where the operational environment is defined by the presence of A2/AD systems and the interdependence of critical infrastructure, space assumes a decisive role. Hybrid warfare activities manifest through jamming and spoofing of satellite communications (Peled, Aizikovich, Habler, Elovici, Shabtai, 2023), cyberattacks against satellite systems (Peled, Aizikovich, Habler, Elovici, Shabtai, 2023), use of kinetic and non-kinetic anti-satellite technologies (Grossfeld, 2024), hostile proximity manoeuvres against Allied satellites (Egeli, 2021), and exploitation of informational ambiguity in space communications to generate strategic confusion (Höyhtyä, Uusipaavalniemi, 2023). These practices undermine confidence in space advantage and place pressure on the ability of the naval forces and NATO to safely integrate space services as part of the space domain in MDO in the Black Sea region.

Cyber Domain

This domain has become indispensable in modern conflict, being doctrinally recognized as a distinct operational environment in which activities of defence, attack, and information exploitation are conducted. NATO has both defined and institutionalized the role of the cyber domain, emphasizing network security and the protection of information flows as essential elements for the success of any joint operation (North Atlantic Treaty Organization, 2019). In US doctrine, operations in cyberspace complement actions in the land, air, maritime, and space environments, ensuring rapid interconnection and resilience, particularly of C2 systems.

In the framework of MDO, the cyber domain serves as the connective tissue linking all other dimensions. MDF rely on the security of digital communications to coordinate actions simultaneously but remain exposed to persistent attacks aimed at degrading networks and compromising informational advantages (US Army Training and Doctrine Command, ib.). Ensuring freedom of action in cyberspace constitutes a decisive factor for maintaining operational tempo and for strengthening interoperability among Allied forces and, implicitly, within multi-domain formations.

In the Black Sea region, hybrid warfare activities targeting the cyber domain are multiple and recurrent. Ransomware6 attacks have already struck critical infrastructure, disrupting the functioning of logistics and transport networks (Schwarz, Marx, Federrath, 2021). Stealth infiltrations7 into naval networks can undermine the detection and reaction capacity of Allied forces (Todorov, 2024), while AI (Artificial Intelligence) – and IoT (Internet of Things)-based automated systems can be manipulated to generate operational confusion (Fenton, 2024). In parallel, disinformation campaigns amplified through cyber channels erode public trust and political cohesion (Usewicz, Keplin, 2023), while DDoS (Distributed Denial of Service) attacks can paralyze C2 centres, limiting multi-domain coordination. These practices undermine regional security and pose major challenges for integrating the naval forces and NATO into a coherent operational architecture in the Black Sea region.

Cognitive/Information Dimension

This dimension is increasingly prominent in the analysis of modern conflicts, reflecting the interdependence between the information environment, decision-making processes, and collective perceptions. While US doctrine does not define it as a standalone domain of MDO, NATO treats it as a connected dimension, indispensable for achieving and maintaining operational advantage, especially in the current context in which Allied states in Eastern Europe face growing challenges in this spectrum. This perspective underscores that victories are not achieved solely through physical manoeuvres but also through the ability to influence the adversary's will and the resilience of one's own societies.

[6] *Ransomware* refers to a type of cyber attack in which an organization's data is encrypted, and access to it is conditional on paying a sum of money to the attacker.

[7] *Stealth infiltration* refers to the discreet and persistent penetration of a computer system, through techniques designed to avoid detection and maintain long-term access.

Regarding MDO, the cognitive dimension supports the integration of the other domains by strengthening legitimacy and preserving cohesion. MDF depend on informational resilience and on the ability to counter adversarial campaigns aimed at the will to fight, trust in institutions, and political stability. Unlike the classical domains: land, air, maritime, space, and cyber, the cognitive/information dimension operates primarily on perceptions, collective memory, and decision-making psychology, which grants it a distinct value in the logic of hybrid confrontations.

With respect to the Black Sea region, this dimension is heavily exploited by the Russian Federation and other actors through hybrid campaigns that include: shaping public discourse via disinformation and propaganda (Deppe, Schaal, 2024), coordinated operations in the digital space combining mass media, social networks, and emerging technologies (Deppe, 2023), algorithmic manipulation and the use of bot networks to amplify false messages (Gombar, 2025), dissemination of strategically targeted fake news to erode trust in institutions (Bârgăoanu, Godzimirski, Ioniță, 2020), and foreign information manipulation and interference (FIMI) campaigns designed to undermine democratic processes and NATO cohesion (Proto, Lamoso-González, García, 2025). These practices create vulnerabilities that are difficult to counter, with direct implications for the implementation of MDO and for regional resilience in the Black Sea.

Civil Cooperation Dimension

The relationship between the military and the civilian environment is a fundamental element of national resilience and of collective defence capacity. NATO doctrine underscores the importance of coordination between military authorities and civilian structures in order to support the conduct of joint operations and to ensure the continuity of essential societal functions (North Atlantic Treaty Organization, 2025). Unlike the doctrinal domains recognized by the US Army Training and Doctrine Command (2018): land, air, maritime, space, and cyber, the relationship with the civilian environment is not defined as a standalone domain of MDO, but is treated instead as a connected dimension, indispensable for implementing MDO in contested environments.

Under MDO architecture, this dimension plays the role of integrating civilian resources and ensuring logistic, energy, and social support for the conduct of operations. Multi-Domain Formations (MDF) rely not only on interoperability among Allied armed forces but also on the ability to employ dual-use civilian infrastructure, to cooperate with national and local authorities, and to sustain public support.

The vulnerability of these relations makes the civil cooperation dimension a primary target of hybrid warfare activities, with the potential to undermine cohesion and erode regional resilience.

Across the Black Sea region, these vulnerabilities are amplified by the strategic context and the proximity of the conflict in Ukraine. Hybrid warfare activities have materialized through the sabotage of critical civilian infrastructure with military relevance (Soldi et al., 2023), cyberattacks against public utility infrastructure with impact on the population and logistics (Fenton, 2024), the exploitation of refugee flows as a tool of political pressure and destabilization (Łubiński, 2022), disinformation campaigns undermining public support for defence, and attacks on dual-use civilian logistics such as ports or transport companies. All these elements highlight that the civil cooperation dimension is vulnerable to hybrid warfare activities, and that protecting this dimension becomes an essential condition for the success of MDO and for maintaining NATO cohesion in the Black Sea region.

HYBRID WARFARE ACTIVITIES IN THE BLACK SEA REGION AND THEIR IMPLICATIONS FOR MDO/MDF

The diversity of hybrid warfare activities requires a careful selection of those that can directly influence the implementation of the MDO doctrine and the establishment of MDF in the Black Sea. The brief description of the domains and dimensions of MDO has shown that they were not delineated by chance, each contributing to the integration and coherence of the operational whole. This section identifies the hybrid warfare threats relevant to each domain/dimension, with implications for the capacity of the naval forces in the Black Sea to implement MDO concepts and, implicitly, MDF, in a strategic environment that is both versatile and contested by the region's main state and non-state actors.

Land Domain (LD)

- *LD1: The use of suicide drones and loitering munitions that affect land mobility and the coastal support of multi-domain operations;*
- *LD2: The sabotage of critical land infrastructure that limits strategic mobility and the logistic support of harbour areas;*
- *LD3: Proxy force operations that generate strategic ambiguity and undermine land security in maritime access areas;*
- *LD4: The disruption of navigation through GNSS jamming that restricts land mobility and the logistic connection with maritime operations;*

- *LD5: The exploitation of international and national legislation aimed at blocking troop deployments and delegitimizing military actions.*

Air Domain (AD)

- *AD1: GNSS jamming and spoofing that affect air navigation and reduce multi-domain synchronization in regional operations;*
- *AD2: Kamikaze drone and loitering munition attacks that saturate defences and diminish the operational capacity of air bases;*
- *AD3: Electromagnetic warfare operations and aerial decoys that degrade radars and reduce the effectiveness of integrated air defence;*
- *AD4: Cyberattacks against air infrastructure that disrupt operations and slow the tempo of multi-domain integration;*
- *AD5: Multi-vector saturation strikes that overwhelm air defence and reduce the resilience of national and Allied air capabilities.*

Maritime Domain (MD)

- *MD1: The sabotage of critical maritime infrastructure that destabilizes logistic and energy chains in the Black Sea;*
- *MD2: The use of unmanned surface vessels (USVs) conducting hard-to-detect offensive attacks against maritime targets;*
- *MD3: AIS and GPS spoofing that distorts ship positioning and creates erroneous perceptions in the maritime domain;*
- *MD4: The obstruction of freedom of navigation by restricting maritime areas declared as naval exercises, with effects on maritime commercial traffic;*
- *MD5: Naval harassment through dangerous manoeuvres and aggressive approaches that intimidate and destabilize safe navigation.*

Space Domain (SD)

- *SD1: Space-based jamming and spoofing that degrade military communications and compromise the synchronization of multi-domain operations;*
- *SD2: Cyberattacks against civilian and military communication satellites that affect Allied operational-strategic responsiveness;*
- *SD3: Kinetic and non-kinetic attacks against satellites that degrade satellite services and disrupt the functioning of the space domain;*
- *SD4: Aggressive proximity manoeuvres in space that compromise satellite integrity and interrupt informational communication networks;*

- *SD5: The exploitation of disinformation and ambiguity regarding space activities that induce uncertainty and erode operational credibility.*

Cyber Domain (CD)

- *CD1: Ransomware attacks against critical infrastructure that block logistic services and disrupt the interoperability of multi-domain operations;*
- *CD2: Disinformation campaigns in cyberspace that erode trust in headquarters and destabilize the information environment;*
- *CD3: Stealth and persistent infiltrations into naval networks that sabotage and hinder Allied detection and response;*
- *CD4: The compromise of AI- and IoT-based automated systems that can be manipulated to generate confusion in the operational domain;*
- *CD5: Coordinated DDoS attacks against command centres that block data transmission to multi-domain formations.*

Cognitive/Information Dimension (CID)

- *CID1: Shaping public discourse through disinformation and propaganda that weaken social cohesion and collective resilience;*
- *CID2: Online information campaigns using mass media, social networks, and emerging technologies to manipulate opinions and behaviours;*
- *CID3: Algorithmic manipulation and bot networks that amplify false messages and generate public opinion polarization;*
- *CID4: Strategically targeted fake news that erodes trust in institutions and undermines rational decision-making processes;*
- *CID5: Foreign information manipulation campaigns that undermine trust in governments and international organizations, affecting the cohesion of alliances and strategic partnerships.*

Civil Cooperation Dimension (CCD)

- *CCD1: The sabotage of civilian infrastructure with military relevance, which limits logistic support and reduces the resilience of multi-domain operations;*
- *CCD2: Cyberattacks against public infrastructure that cause major disruptions and affect the support of military operations;*
- *CCD3: The exploitation of refugee flows and forced migration as instruments of political pressure and social destabilization;*
- *CCD4: Disinformation campaigns that manipulate public perceptions and reduce civilian support for collective defence initiatives;*

- *CCD5: Attacks on dual-use civilian logistics that affect infrastructure essential both for commercial flows and for military support.*

MULTI-CRITERIA COMPARATIVE ANALYSIS OF THE IMPLICATIONS OF HYBRID WARFARE ACTIVITIES ON MDO AND MDF IN THE BLACK SEA REGION

The application of the methodology involves transforming the identified threats into comparative assessment instruments, in order to highlight how they affect multi-domain operations and the capacity of MDF to be constituted and to operate in the Black Sea region. Each domain has been analysed in relation to five characteristic threats, synthesized into short versions to facilitate their integration into a common analytical framework. The domains have been assessed based on three criteria: intensity (I), probability (P), and relevance (R) for MDF, each with values ranging from 1 to 5. The resulting scores do not represent mere numerical values but rather the outcome of a critical interpretative process designed to capture the interaction and interdependence between vulnerabilities and multi-domain response options.

Table 1: Assessment of the implications of hybrid warfare activities on the land domain

Hybrid warfare activities – land domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
LD1: Use of drones and loitering munitions	5	4	5	14	Reduce coastal protection capacity and expose naval logistic support lines
LD2: Sabotage of critical land infrastructure	4	4	5	13	Delay replenishment and restrict the freedom of manoeuvre of naval support
LD3: Proxy force operations	3	5	4	12	Weaken Allied coordination and endanger land support lines for naval forces
LD4: Land-based GNSS jamming	4	4	4	12	Hinder land manoeuvres and reduce the efficiency of coordination with naval support
LD5: Exploitation of legislation	3	3	4	10	Delay military response and reduce the freedom of action of joint naval operations

Hybrid warfare activities – land domain	**I**	**P**	**R**	**Total**	**Implications for the MDO of naval forces in the Black Sea**
Average score for the land domain	**12.2 / 15**				

In *table 1*, the main hybrid warfare activities affecting the land domain are presented, with emphasis on the use of drones, the sabotage of logistic infrastructure, and the infiltration of proxy forces. The high scores indicate that the vulnerability of infrastructure and transport routes can restrict the freedom of manoeuvre of naval forces and undermine the capacity of MDF to sustain coastal operations and to operate effectively in the land support area adjacent to the littoral.

Table 2: Assessment of the implications of hybrid warfare activities on the air domain

Hybrid warfare activities – air domain	**I**	**P**	**R**	**Total**	**Implications for the MDO of naval forces in the Black Sea**
AD1: GNSS jamming and spoofing	4	4	5	13	Disrupt air missions and limit reconnaissance and fire support for naval forces
AD2: Kamikaze drone and loitering munition attacks	5	4	5	14	Weaken air support and reduce the freedom of manoeuvre of naval operations
AD3: Electromagnetic warfare operations	4	4	5	13	Undermine air defence and expose naval forces to coordinated strikes
AD4: Cyberattacks against air infrastructure	4	3	4	11	Delay air support and affect the courses of action of naval forces
AD5: Multi-vector saturation strikes	5	3	5	13	Exhaust air defence and leave naval forces exposed to successive attacks
Average score for the air domain	**12.8 / 15**				

In *table 2*, the main hybrid warfare activities affecting the air domain are presented, among which GNSS jamming and spoofing, kamikaze drone attacks, and multi-vector strikes register the highest scores. These activities can disrupt air missions, limit ISR (Intelligence, Surveillance and Reconnaissance) support, and reduce air defence protection, critical aspects for covering naval forces and for their integration into MDO in the Black Sea.

Table 3: Assessment of the implications of hybrid warfare activities on the maritime domain

Hybrid warfare activities – maritime domain	**I**	**P**	**R**	**Total**	**Implications for the MDO of naval forces in the Black Sea**
MD1: Sabotage of critical infrastructure	5	4	5	14	Disrupt essential energy and logistic flows supporting naval operations
MD2: Use of unmanned surface vessels	5	4	5	14	Threaten ship security and reduce freedom of navigation in coastal areas
MD3: AIS and GPS spoofing	4	4	5	13	Induce navigation errors, simulate illegal entries into TTW (territorial waters), and increase the risk of maritime incidents
MD4: Restriction of freedom of navigation	4	4	5	13	Limit freedom of navigation and reduce maritime mobility of Allied forces in the region
MD5: Naval harassment through dangerous manoeuvres	4	4	5	13	Increase the risk of collisions, diplomatic incidents, and undermine the security of Allied naval and maritime operations
Average score for the maritime domain	**13.4 / 15**				

In *table 3*, the main hybrid warfare activities affecting the maritime domain are presented, with high values assigned to the sabotage of critical maritime infrastructure and naval drone attacks. Other activities, such as AIS/GPS spoofing, restrictions on freedom of navigation, and naval harassment, highlight the vulnerability of freedom of navigation and the security of maritime operations in the Black Sea, particularly in the current context of the Russia-Ukraine conflict, when the presence of Allied naval forces is largely limited to maritime patrol aircraft missions.

Table 4: Assessment of the implications of hybrid warfare activities on the space domain

Hybrid warfare activities – space domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
SD1: Space-based jamming and spoofing	4	4	5	13	Disrupt navigation and reduce C2 coherence between naval and Allied components
SD2: Satellite cyberattacks	4	3	5	12	Weaken naval communications and delay synchronization of multi-domain operations
SD3: Attacks against satellites	5	2	5	12	Reduce GPS accuracy and limit the informational support of naval forces
SD4: Aggressive proximity manoeuvres in space	4	3	4	11	Reduce the reliability of satellite communications and affect naval operational coordination
SD5: Disinformation and ambiguity regarding space activities	3	4	4	11	Delay decision-making and reduce the operational cohesion of naval forces.
Average score for the space domain	**11.8 / 15**				

In *table 4*, the main hybrid warfare activities affecting the space domain are presented, among which jamming and spoofing, cyberattacks, and proximity manoeuvres register significant scores. These activities can affect satellite communications, navigation, and the synchronization of multi-domain operations, particularly in the maritime domain, where satellite services are essential for precise positioning and for the guidance of munitions trajectories during enemy engagement.

Table 5: Assessment of the implications of hybrid warfare activities on the cyber domain

Hybrid warfare activities – cyber domain	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CD1: Ransomware attacks	4	4	5	13	Hinder logistic chains and reduce the reaction speed of naval forces
CD2: Disinformation campaigns in cyberspace	3	4	4	11	Undermine trust in C2 and reduce the operational cohesion of naval forces
CD3: Cyber infiltrations	4	4	5	13	Compromise information security and limit the effectiveness of joint naval defence
CD4: Compromise of automated systems	3	4	4	11	Disrupt digital architectures and reduce the predictability of multi-domain naval operations
CD5: DDoS attacks	4	4	5	13	Paralyze C2 flows and delay the reaction of naval forces
Average score for the cyber domain	**12.2 / 15**				

In *table 5*, the main hybrid warfare activities affecting the cyber domain are presented, with emphasis on ransomware attacks, persistent infiltrations, and DDoS attacks. These activities can compromise information security, disrupt C2 flows, and affect naval coordination in multi-domain operations, thereby reducing the reaction speed and resilience of MDF of the naval forces in the Black Sea.

Table 6: Assessment of the implications of hybrid warfare activities on the cognitive/information dimension

Hybrid warfare activities – cognitive/information dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CID1: Disinformation and propaganda	3	5	4	12	Erode public support and reduce the legitimacy of naval multi-domain actions

Hybrid warfare activities – cognitive/information dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CID2: Manipulative information campaigns	3	4	4	11	Distort collective perceptions and reduce public backing for joint naval operations
CID3: Manipulation through algorithms and bot networks	3	4	4	11	Undermine internal cohesion and reduce political support for implementing MDO in the Black Sea region
CID4: Strategically targeted fake news	3	4	4	11	Weaken trust in institutions and reduce public support for multi-domain operations
CID5: Foreign manipulation campaigns	4	3	5	12	Reduce Allied cohesion and weaken international support for establishing naval MDF in the Black Sea
Average score for the cognitive/information dimension	**11.4 / 15**				

In *table 6*, the main hybrid warfare activities affecting the cognitive and information dimension are presented, such as disinformation, manipulation through algorithms and bot networks, and strategically targeted fake news. These activities can erode social cohesion, trust in institutions, and public support for multi-domain operations, with an indirect impact on the legitimacy of Allied naval presence and on the political support for the establishment and implementation of MDF in the Black Sea region.

Table 7: Assessment of the implications of hybrid warfare activities on the civil cooperation dimension

Hybrid warfare activities – civil cooperation dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CCD1: Sabotage of civilian infrastructure with military relevance	5	4	5	14	Disrupt replenishment and reduce the resilience of support for multi-domain operations in the Black Sea

Hybrid warfare activities – civil cooperation dimension	I	P	R	Total	Implications for the MDO of naval forces in the Black Sea
CCD2: Cyberattacks against civilian infrastructure	4	4	4	12	Delay naval logistic support and affect the continuity of MDF operations in the region
CCD3: Exploitation of refugee flows and forced migration	3	4	3	10	Overstretch state resources and reduce the capacity to support MDF
CCD4: Disinformation campaigns	3	4	4	11	Reduce public acceptance of MDO implementation and delegitimize naval operations in the region
CCD5: Attacks on dual-use civilian logistics	4	4	5	13	Delay naval replenishment and limit the resilience of operational support in the Black Sea
Average score for the civil cooperation dimension	**12.0 / 15**				

In *table 7*, the main hybrid warfare activities affecting the civil cooperation dimension are presented, among which the sabotage of infrastructure, attacks on dual-use logistics, and disinformation campaigns register the highest scores. These activities can affect naval replenishment flows, the operating patterns of MDF, and public support for collective defence initiatives, underscoring the critical interdependence between the civilian and military sectors in the Black Sea region.

Table 8: Comparison of average scores across MDO domains and dimensions

Domain/Dimension	Average score (maximum 15)
LD - Land	12.2
AD - Air	12.8
MD - Maritime	13.4
SD - Space	11.8
CD - Cyber	12.2
CID - Cognitive/Information	11.4
CCD - Civil cooperation	12.0

In *table 8*, the average scores obtained for each analysed domain and dimension are synthesized. The results indicate that the maritime domain, in the Black Sea region, as part of multi-domain operations, faces the highest level of vulnerability to hybrid activities (13.4/15), followed by the air, land, and cyber domains, which directly support freedom of manoeuvre and the security of logistic flows. The space domain and the cognitive/information dimension, although recording lower values, generate significant cross-cutting effects, affecting multi-domain coordination and the legitimacy of Allied actions, particularly with regard to naval forces. At the same time, the civil cooperation dimension confirms the importance of critical and dual-use infrastructure, as well as social cohesion, for the operational resilience of MDF. This distribution of vulnerabilities constitutes the starting point for the integrated analysis of the results, in which the interdependence among domains becomes decisive for the success of multi-domain operations in the Black Sea region.

RESULTS

The application of the multi-criteria comparative analysis made it possible to transpose into a unified framework the thirty-five hybrid warfare activities identified for each domain/dimension as part of multi-domain operations. The results highlight significant differences between domains, as well as common trends with direct relevance for the capacity of the naval forces and NATO to constitute and operate MDF in the Black Sea region.

The highest level of vulnerability is found in the maritime domain (13.4/15), a fact explained by the concentration of threats against critical port infrastructure, the use of autonomous naval drones, and the restriction of freedom of navigation. This vulnerability is amplified by the context of the Russia-Ukraine conflict, in which the maritime domain directly supports land operations and provides the Russian Federation with a significant geographic advantage. The proximity of the Black Sea to Russian territory transforms this space into a strategic depth for Romania, at NATO's southeastern boarder, which intensifies the pressure on maritime security and freedom of navigation. The air domain ranks immediately after the maritime one, being exposed to GNSS jamming, kamikaze drone attacks, and multi-vector strikes, factors that reduce ISR support and the air defence protection necessary for naval operations. The land and cyber domains, located on the same risk tier (12.2/15), confirm the importance of logistics and information security: sabotage of infrastructure, persistent infiltrations, and ransomware attacks can block replenishment and disrupt C2 flows, diminishing the reaction capacity of MDF.

The civil cooperation dimension (12.0/15) underscores the critical interdependence between dual-use infrastructure and societal resilience, both indispensable for supporting the establishment and operation of MDF at the level of naval forces and for the public acceptance of Allied presence in the Black Sea region.

The lower scores recorded for the space domain (11.8/15) and the cognitive/information dimension (11.4/15) do not reflect a lack of relevance but rather their cross-cutting character. Jamming and attacks against satellites can simultaneously compromise navigation, communications, and cross-domain coordination, while information manipulation and the erosion of social cohesion can undermine legitimacy and the Allied decision-making capacity to sustain naval operations in the Black Sea. Overall, the results confirm the working hypothesis stated in the introduction, demonstrating that hybrid warfare activities produce asymmetric effects across domains, being particularly pronounced in the maritime domain, while at the same time manifesting through multiple interdependencies, with a cumulative effect on the implementation of multi-domain operations.

With regard to the limitations of the research, the analysis is based on data collected from open sources, which excludes both classified information and the lessons learned from NATO exercises in the Black Sea region or from the ongoing Russia-Ukraine conflict, as these cannot be fully documented through public sources. Secondly, the applied multi-criteria method provides a prospective perspective, useful for planning, but one that requires empirical validation through scenarios and wargaming exercises. Finally, the scores assigned to the implications of hybrid warfare activities may reflect a degree of subjectivity at the time of assessment, since they have been established on the basis of the available academic and doctrinal literature. These limitations do not diminish the value of the results but instead indicate future directions of research and justify the need for doctrinal and operational recommendations that address the research question set out in the introduction.

In this regard, the analysis provides a comparative framework that serves as the foundation for the conclusions and adaptation proposals formulated in the paper, oriented toward strengthening the capacity to implement the MDO doctrine and MDF in the Black Sea region.

CONCLUSIONS

The results obtained through the multi-criteria comparative analysis highlight that the maritime domain is the most vulnerable to hybrid warfare activities, followed by the air domain, while the land and cyber dimensions confirm the critical role of logistics and information security in supporting operations in the Black Sea region.

The space domain and the cognitive/information dimension, although recording lower scores, generate significant cross-cutting effects, while the civil cooperation dimension underscores the interdependence between critical infrastructure and social cohesion with operational resilience. These findings enable the formulation of an integrated response to the research question: *How do hybrid warfare activities affect the capacity of the naval forces in the Black Sea to implement MDO by the 2030 horizon, and what doctrinal, technological, and organizational adaptations are required for multi-domain formations?* Within this framework, the analysis has shown that hybrid warfare activities manifest in the logic of interdependence among domains/dimensions, with a cumulative effect on the implementation of the MDO doctrine and MDF in the Black Sea region.

The analysis has demonstrated that hybrid warfare activities employ a direct and disproportionate influence on the capacity to implement multi-domain operations in the Black Sea region. The maritime domain emerges as the most exposed, since freedom of navigation, the security of critical maritime infrastructure, and the protection of SLOC can be undermined by sabotage, naval drone attacks, or deliberate naval harassment. Vulnerabilities in the air domain amplify these risks by limiting ISR support and air defence protection, which in turn reduces the level of coordination and delays the reaction capacity of naval forces in the Black Sea.

At the same time, the land and cyber domains confirm that logistics and the security of information flows are essential elements for sustaining MDF. The sabotage of transport routes, proxy infiltrations, ransomware cyberattacks, or the compromise of C2 networks can block naval support and compromise the temporal coordination of naval operations. The space domain and the cognitive/information dimension, although scoring lower in the comparative analysis, generate cross-cutting effects with major impact: jamming and attacks against satellites can degrade navigation and communications, while information manipulation and the erosion of social cohesion undermine political legitimacy and public support. Equally, the civil cooperation dimension highlights the critical dependence of the naval forces on dual-use infrastructure and social resilience, without which freedom of manoeuvre and operational continuity cannot be ensured.

Therefore, hybrid warfare activities affect not only an isolated domain but the entire architecture of multi-domain operations, through a logic of interdependencies and cumulative effects. This reality demonstrates that the success of implementing MDF in the Black Sea region depends simultaneously on the protection of critical infrastructure, the safeguarding of information security, and the assurance of freedom of navigation.

To address the second part of the research question, it is necessary to identify doctrinal, technological, and organizational adaptations through which the naval forces can strengthen their resilience against hybrid warfare activities and ensure the effective implementation of MDF in the Black Sea region. Within this framework, the research has highlighted seven priority directions of action, with practical and forward-looking value, aimed at transforming theoretical results into concrete operational recommendations:

- the development of naval capabilities dedicated to the detection and neutralization of autonomous maritime drones, as well as to countering underwater sabotage, in order to protect critical infrastructure and SLOC;
- the development of naval capabilities equipped with automated short and medium-range air and missile defence systems, designed to intercept threats in the proximity of the maritime area and to transfer them to land-based long-range defence systems, with the aim of protecting MDF and, implicitly, national territory;
- the implementation of integrated protection mechanisms for dual-use infrastructure, such as harbours, energy networks, and transportation systems, through dedicated cooperation plans agreed at the interagency level;
- the adaptation of naval force training and MDF components for hybrid-type scenarios, by integrating them into training programs and into national and multinational exercises;
- the design of naval MDF as flexible and modular entities, capable of integrating land, naval, air, and cyber actions into a unified framework adapted to the specific security environment of the Black Sea;
- the integration of MDF into NATO's regional structures, with emphasis on the role of Romania and Bulgaria as littoral states and strategic staging points for operations in the Black Sea;
- the allocation of dedicated satellite support through the allocation of military satellites for naval MDF in the Black Sea, with redundancy mechanisms to ensure the continuous functioning of C2 systems and the sustained support of combat structures as integral components of MDF.

The recommendations formulated are aligned with the DOTMLPFI (Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Interoperability) framework and outline an initial, coherent adaptation plan for the naval forces and NATO in the Black Sea region. At the doctrinal level, MDO must be established as an operational-strategic foundation, while for MDF it is necessary to elaborate dedicated manuals and tactical procedures. From an organizational perspective, priority should be given to the creation of flexible naval structures and their integration into NATO's regional architecture. In the field of training, scenarios of hybrid warfare activities must be systematically integrated into national and multinational exercises, with emphasis on ensuring freedom of navigation in the Black Sea. In terms of equipment, investments in counter-drone systems, anti-jamming capabilities, and redundant satellite assets are vital for safeguarding C2 resilience and freedom of navigation. Leadership requires strengthening through interdisciplinary training programs, and personnel must be selected and prepared to operate effectively at the fine intersection of MDO domains and dimensions. With regard to infrastructure, the modernization and maintenance of dual-use facilities such as harbours, energy nodes, and logistics hubs at high standards becomes essential for operational support. Finally, technological and procedural interoperability must be reinforced to efficiently integrate MDF into the Allied architecture. Thus, the success of implementing multi-domain formations in the Black Sea depends on an integrated transformation that combines doctrinal, organizational, technological, and social dimensions into a unified framework of resilience and adaptation.

BIBLIOGRAPHY:

1. Allied Command Transformation (24 August 2025). *Allied Command Transformation*, Multi-Domain Operations Conferences: https://www.act.nato.int/activities/multi-domain-operations/?utm_source=chatgpt.com, retrieved on 30 August 2025.
2. Bachmann, S.D., Mosquera, A.M. (2015). *Lawfare and hybrid warfare – how Russia is using the law as a weapon. The Military Law and the Law of War Review*, pp. 45-58, https://journals.sas.ac.uk/amicus/article/view/2433/2395, retrieved on 30 August 2025.
3. Batyuk, V. (3 September 2017). *The US concept and practice of hybrid warfare. Strategic Analysis, 41*(5), pp. 464 - 477. doi:10.1080/09700161.2017.1343235.
4. Bârgăoanu, A., Godzimirski, J., Ioniță, D. (2020). *Information warfare and information operations in The Black Sea area.* (N. S. Center, Ed.), newstrategycenter.ro: https://www.newstrategycenter.ro/wp-content/uploads/2019/11/FLANKS-Working-Paper-Information-Warfare-And-Information-Operations-in-the-Black-Sea-Area.pdf, retrieved on 12 August 2025.
5. Beznosiuk, M. (25 August 2025). *Atlantic Council,* Putin's hybrid war against Europe continues to escalate: https://www.atlanticcouncil.org/blogs/ukrainealert/putins-hybrid-war-against-europe-continues-to-escalate, retrieved on 25 August 2025.
6. Burlacu, P., Sandu, M.V. (2023). *Ukrainian USV (Uncrewed Surface Vessel) attack on ships of the Black Sea Fleet Lessons learned*. (M. P. Constanta, Ed.) *Scientific Bulletin of Naval Academy, XXVI 2023*(2), pp. 31-40. doi:10.21279/1454-864X-23-I2-003.
7. Creswell, J., Creswell, D. (2018). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (5th ed., Vol. 1). California: SAGE Publications, Inc., https://spada.uns.ac.id/pluginfile.php/510378/mod_resource/content/1/creswell.pdf, retrieved on 20 August 2025.

8. Cucinschi, A.L. (2024). *The Suitability of Multi-Domain Operations for the Black Sea* (A.L. Reczkowski, Ed.). *GLOBSTATE Responding to contemporary challenges in security and operating environments strategy, operations, methodology, 6*(1), pp. 75-85, doi:https://cdissz.wp.mil.pl/u/documents/Responding_to_Contemporary_Challenges_in_Security_and_Operating_Environments_-_online_print_off_PGVURm1.pdf, retrieved on 22 August 2025.
9. Dalsjö, R., Jonsson, M., Norberg, J. (30 May 2022). *A Brutal Examination: Russian Military Capability in Light of the Ukraine War*. *Survival: Global Politics and Strategy, 64*(3), pp. 7-28. doi:10.1080/00396338.2022.2078044.
10. Deppe, C. (2023). *Disinformation in Cognitive Warfare Foreign Information Manipulation and Interference, and Hybrid Threats.* doi:10.5281/zenodo.10005172
11. Deppe, C., Schaal, G. (2024). *Cognitive warfare: a conceptual analysis of the NATO ACT cognitive warfare exploratory concept.* doi:10.3389/fdata.2024.1452129.
12. Eckel, M. (20 August 2025). *Report: Russian Sabotage Operations in Europe Have Quadrupled Since 2023,* Radio Free Europe/Radio Liberty: https://www.rferl.org/a/russia-sabotage-europe-hybrid-attacks/33508179.html, retrieved on 24 August 2025.
13. Egeli, S. (25 June 2021). *Space-to-Space Warfare and Proximity Operations: The Impact on Nuclear Command, Control, and Communications and Strategic Stability.* doi:10.1080/25751654.2021.1942681.
14. Fenton, A.J. (19 March 2024). *Preventing Catastrophic Cyber-Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore.* doi:10.3390/jmse12030510.
15. Ferris, J. (2012). *Small wars and great games: The British Empire and hybrid warfare, 1700-1970*. In J. Ferris, *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Vol. 1, pp. 199-224). Cambridge University Press. doi:10.1017/CBO9781139199254.008.
16. Florido-Benítez, L. (2024, 08 28). *The types of hackers and cyberattacks in the aviation industry*. In *Journal of Transportation Security, 17*. doi:10.1007/s12198-024-00281-9.
17. Gaber, Y. (2024). *A New Security Reality Strategic Approaches for the Wider Black Sea Region,* George C. Marshall European Center For Security Studies: https://www.marshallcenter.org/sites/default/files/files/2024-11/gaber_a-new-security-reality-clock-tower-final_20241105_1.pdf, retrieved on 21 August 2025.
18. Godzimirski, J., Mitrescu, S. (29 May 2025). *HYBRID FRONTLINES: Russian Threats and the Future of Maritime Infrastructure in the Black Sea and the North Sea.* (G. Scutaru, Ed.), caleaeuropeana.ro: https://www.caleaeuropeana.ro/wp-content/uploads/2025/05/WP1_versiune-finala-macheta.pdf, retrieved on 23 August 2025.
19. Gombar, M. (3 March 2025). *Algorithmic Manipulation and Information Science: Media Theories and Cognitive Warfare in Strategic Communication,* ej-media.org: https://www.ej-media.org/index.php/media/article/view/41/59, retrieved on 12 August 2025.
20. Grier, P. (2017). *The perils of hybrid wars*. In *Air Force Magazine, 100*(3), pp. 24- 29, https://0k11m85ld-y-https-www-scopus-com.z.e-nformation.ro/pages/publications/85019186186, retrieved on 23 August 2025.
21. Grossfeld, E. (2024). *Russia's Declining Satellite Reconnaissance Capabilities and Its Implications for Security and International Stability.* (Routledge) doi:10.1080/08850607.2024.2330848.
22. Headquarters, Department of the Army (2025). *FM 3-0 Operations.* Department of the Army. Department of the Army, https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN43326-FM_3-0-000-WEB-1.pdf, retrieved on 22 August 2025.

23. Hoehn, J. (2021). *Joint All-Domain Command and Control (JADC2).* Congressional Research Service. Congress.gov., https://www.congress.gov/crs_external_products/IF/PDF/IF11493/IF11493.14.pdf, retrieved on 23 August 2025.
24. Höyhtyä, M., Uusipaavalniemi, S. (2023). *The space domain and the Russo-Ukrainian war: Actors, tools, and impact.* (H. CoE, Ed.), Hybrid CoE: https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230109-Hybrid-CoE-Working-Paper-21-Space-and-the-Ukraine-war-WEB.pdf, retrieved on 14 August 2025.
25. Islam, M. (2024). *Maritime Diplomacy and Regional Cooperation Mechanisms: Insights from the Black Sea and Bay of Bengal*. *Millennial Asia*. doi:10.1177/09763996241256162.
26. Kohler, M. (2020). *The Joint Force Maritime Component Command and the Marine Corps Integrate to Win the Black Sea Fight*. In *Journal of Advanced Military Studies, 11*(2), pp. 88-105. doi:10.21140/mcuj.20201102005.
27. Kunertova, D. (2023). *Drones have boots: Learning from Russia's war in Ukraine*. *CONTEMPORARY SECURITY POLICY, 44*(4), pp. 576-591. doi:doi.org/10.1080/13523260.2023.2262792
28. Łubiński, P. (2022). *Hybrid Warfare or Hybrid Threat – The Weaponization of Migration as an Example of the Use of Lawfare – Case Study of Poland*. *Polish Political Science Yearbook, 51*, pp. 43-55. doi:10.15804/ppsy202208.
29. Mitrescu, S., Sokolov, M. (2025). *In the Crosshairs: Hybrid Threats and the Challenge to Maritime Infrastructure*. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pp. 65-90). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_6.
30. Monaghan, A., Connolly, R. (2023). *The sea in Russian strategy* (Vol. 1). Manchester: Manchester University Press.
31. North Atlantic Treaty Organization (February 2019). *Allied Joint Doctrine for the Conduct of Operations (AJP*-3). *(1), C*, 164. NATO Standardization Office, https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf, retrieved on 22 August 2025.
32. North Atlantic Treaty Organization (June 2025). AJP-3.19, Allied Joint Doctrine for civil-military cooperation. *NATO Standardization Office (NSO)(1), B*, 62. NATO Standardization Office (NSO), https://www.coemed.org/files/stanags/01_AJP/AJP-3.19_EDA_V1_E_2509.pdf, retrieved on 22 August 2025.
33. Orde, K. (2016). *Lawfare: Law as a Weapon of War.* Oxford University Press. doi:10.1093/acprof:oso/9780190263577.001.0001.
34. Peled, R., Aizikovich, E., Habler, E., Elovici, Y., & Shabtai, A. (2023). *Evaluating the Security of Satellite Systems*, arxiv.org: https://arxiv.org/pdf/2312.01330, retrieved on 12 August 2025.
35. Plichta, M. (2025). *Precise Mass in Action. Assessing Ukraine's One-Way Attack Drone Campaign*. *RUSI, 170*(4), pp. 42-48. doi:10.1080/03071847.2025.2527923.
36. Proto, L., Lamoso-González, P., García, L.B. (2025). *The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight.* doi:10.17645/mac.9474.
37. Sabanadze, N., Dalay, G. (2025). *Understanding Russia's Black Sea strategy. How to strengthen Europe and NATO's approach to the region*, Chatham House: https://www.chathamhouse.org/2025/07/understanding-russias-black-sea-strategy/03-threat-perceptions-and-failure-signalling, retrieved on 22 August 2025.
38. Schaub, G., Murphy, M., Hoffman, F. (2017). *Hybrid maritime warfare building Baltic resilience.* In *RUSI Journal, 162*(1), pp. 32-40. doi:10.1080/03071847.2017.1301631.

39. Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). *A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. ACM Computing Surveys (CSUR), 48*(4), pp. 1-31. doi:https://doi.org/10.1145/2897166.
40. Schwarz, M., Marx, M., Federrath, H. (2021). *A Structured Analysis of Information Security Incidents in the Maritime Sector.* doi:10.48550/arXiv.2112.06545.
41. Scutaru, G., Pavel, A. (2025). *Black Sea Region Security Assessment*. In *NATO Science for Peace and Security Series C: Environmental Security* (Vol. Part F140, pp. 29-38). Springer Science and Business Media B.V. doi:10.1007/978-94-024-2300-6_3.
42. Soldi, G., Gaglione, D., Rapone, S., Forti, N., d'Afflisio, E., Kowalski, P., ... Warner, C. (2023). *Monitoring of Underwater Critical Infrastructures: the Nord Stream and Other Recent Case Studies.* doi:10.48550/arXiv.2302.01817.
43. Stensrud, C.J., Østhagen, A. (2024). *Hybrid Warfare at Sea? Russia, Svalbard and the Arctic*. In *Scandinavian Journal of Military Studies, 7*(1), pp. 111-130. doi:10.31374/sjms.233.
44. Tagarev, T. (2021). *Understanding Hybrid Influence: Emerging Analysis Frameworks*. *Studies in Big Data, 84*, pp. 449-463. doi:10.1007/978-3-030-65722-2_29.
45. Todorov, Y. (2024). *Navigating Uncharted Waters: Tackling Maritime Cybersecurity Challenges in the Black Sea Region*. *Information & Security, 55*(2), 113-132. doi:10.11610/isij.5509.
46. US Air Force (2021). Air Force Doctrine Publication 1: The Air Force. *Air Force Doctrine Publication 1: The Air Force, 1, 1*, 20. Center for Doctrine Development and Education, https://www.doctrine.af.mil/Portals/61/documents/AFDP_1/AFDP-1.pdf, retrieved on 22 August 2025.
47. US Army Training and Doctrine Command (2018). The U.S. Army in Multi-Domain Operations 2028 (TRADOC Pamphlet 525-3-1). 100. TRADOC, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf, retrieved on 12 August 2025.
48. US Navy (2025). SURFACE WARFARE: THE COMPETITIVE EDGE 2.0. *SURFACE WARFARE: THE COMPETITIVE EDGE 2.0, 1, 2*, 32. Commander, Naval Surface Force, US Pacific Fleet, https://www.surfpac.navy.mil/Portals/54/Documents/CNSP/SNA/SNA-2025/THE%20COMPETITIVE%20EDGE%202.0%20Jan%203%20Print%20Final.pdf, retrieved on 20 August 2025.
49. US Space Force (2025). Space Force Doctrine Document – 1 (SFDD-1), The Space Force. *(1), 1*, 51. Space Training and Readiness Command (STARCOM), https://www.starcom.spaceforce.mil/Portals/2/Space%20Force%20Doctrine%20Document%201%20FINAL_4Apr25.pdf, retrieved on 20 August 2025.
50. Usewicz, T., Keplin, J. (2023). *Hybrid Actions and Their Effect on EU Maritime Security*. In *Journal on Baltic Security, 9*(1), pp. 32-68. doi:10.57767/jobs_2023_001.
51. Vdovychenko, V., Albu, N., Chitadze, N. (2024). *Navigating the Trilemma of (In) security: Strategic Competition in the Black Sea Region*. *Center for Defence Strategies, Ukraine, 23*(2), pp. 117-128. doi:10.11610/Connections.23.2.08.
52. Wither, J. (2023). *Hybrid Warfare Revisited: A Battle of 'Buzzwords'*. *Connections, 22*(1), pp. 7-27. doi:10.11610/Connections.22.1.02.
53. Zorri, D., Kessler, G. (2024). *Position, Navigation, and Timing Weaponization in the Maritime Domain: Orientation in the Era of Great Systems Conflict,* National Defense University Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678180/position-navigation-and-timing-weaponization-in-the-maritime-domain-orientation, retrieved on 22 August 2025.