



HYBRID THREATS IN THE BLACK SEA – IDENTIFYING GEOGRAPHIC AND ECONOMIC VULNERABILITIES OF ROMANIA’S MARITIME AREA –

Navy Commander Instructor Valentin-Costinel TOTIR, PhD Candidate

“Carol I” National Defence University

Navy Captain (r.) Professor Ion CHIORCEA, PhD

“Mircea cel Bătrân” Naval Academy

10.55535/RMT.2024.1.5

With no clear evidence of its origin, hybrid warfare is a worldwide phenomenon, its effects having worldwide reverberations. Characterised by a very high adaptability and flexibility of the methods and procedures used, as well as the continuous expansion of the target audience or the area of coverage, hybrid warfare is not a new concept in human history. Overshadowed by the much higher degree of destruction and the very large number of human victims – specific to conventional war – unconventional actions – an integral part of hybrid war – often go unnoticed, but their effects are felt in all areas of human society existence. Today, the annexation of Crimea and the invasion of Ukraine by the Russian Federation are classic examples of hybrid warfare, characterised by true intentions concealment along with the fact that special operations forces experience and support allowed ethnic Russian communities to organise paramilitary groups with the aim of creating an ambiguous and insecure environment on Ukraine’s territory.

Furthermore, these events forced NATO leaders to identify and implement measures to limit and reduce Russian Federation possibilities to apply a similar strategy against the Black Sea or Baltic Sea member states. Analysing in detail the Russian hybrid actions major impact in the maritime environment, materialised both by the two parties’ state borders modification and the Russian Federation Exclusive Economic Zone expansion to the detriment of Ukraine, this paper aims to identify geographical and economic vulnerabilities in the Black Sea, the exploitation of which can result in the weakening of the south-eastern flank of the North Atlantic Alliance. Moreover, the present study’s results will represent the basis of a further analysis that will highlight the optimal measures for their reduction.

Keywords: hybrid warfare; hybrid maritime warfare; hybrid threats; hybrid maritime threats; maritime vulnerabilities;



INTRODUCTION

Benefiting from the support of Russian ethnic communities, the hybrid actions of the Russian Federation have had the common purpose of paralysing the Ukrainian decision-making process by creating an ambiguous environment and concealing true intentions. Furthermore, the experience and support of special operations forces have allowed Russian ethnic communities to organise paramilitary groups and provide information regarding the disposition of major conventional capabilities, with the aim of deterring foreign intervention in support of the Ukrainian armed forces (Murphy, Hoffman, & Schaub, Warfare and the Baltic Sea Region, 2016, p. V; English Abstract).

The use of hybrid warfare techniques by the Russian Federation throughout the entire conflict with Ukraine has had a significant impact on the security environment in Europe, with global repercussions.

Today, there are state and non-state actors challenging nations, institutions, and private companies through a wide range of overt and covert activities targeting their vulnerabilities. Both NATO and the European Union refer to these as “*hybrid threats*”, and the maritime domain has proven to be particularly vulnerable.

The term *hybrid* refers to actions that can be conducted by any state, as well as a variety of non-state actors. These involve multi-modal activities and actions that can be carried out by separate units or even the same unit but are generally directed and coordinated at various levels throughout the battlespace to achieve synergistic effects in the physical and psychological domains.

Essentially, the key aspect of hybrid threats is the deliberate “*blurring and mixing*” of adversarial organisational forms, types of weapons, and tactics used, often at or beyond the legal boundaries, directed at military or civilian targets, with the dual purpose of weakening the adversary’s resilience and creating an advantage for one’s own or allied forces.

The key aspect of hybrid threats is the deliberate “blurring and mixing” of adversarial organisational forms, types of weapons, and tactics used, often at or beyond the legal boundaries, directed at military or civilian targets, with the dual purpose of weakening the adversary’s resilience and creating an advantage for one’s own or allied forces.



Within the maritime environment, among the vulnerabilities that a potential adversary could exploit there are latent disputes over territorial waters with implications for fishing rights in particular and the exploitation of the maritime environment in general.

The maritime dimension of vulnerability for states with access to the sea has received inadequate attention, particularly in NATO's evolving response to hybrid threats. There are ports and coastal areas with pro-Russian populations that, at some point, could serve as an initiation point for disturbances affecting national security and safety.

Within the maritime environment, among the vulnerabilities that a potential adversary could exploit there are latent disputes over territorial waters with implications for fishing rights in particular and the exploitation of the maritime environment in general.

This work aims to analyse Romania's area of responsibility in the Black Sea and to identify a series of geographic and economic vulnerabilities that, if efficiently exploited, could affect the country's security. Furthermore, the sea can be characterised as a theatre where hybrid actions could prevail, for countering which a judicious analysis of these vulnerabilities is necessary. This subject could form the central element of a subsequent scientific endeavour, the result of which would materialise in the identification of potential responses to reduce risks and enhance the resilience of states bordering a closed or semi-enclosed sea.

In fulfilling the purpose of this scientific undertaking, we believe it is essential to understand the peculiarities of hybrid warfare in the maritime environment, as well as to realise that the geographic characteristics and economic importance of the Black Sea's resources, when not adequately managed, transform into vulnerabilities that can materialize as hybrid threats to the state's security and safety.

MARITIME HYBRID THREATS

Recognising from very early on that the struggle for survival, both as individuals and as a species, is governed by violence, human society has understood the importance of establishing and enforcing a regulatory framework governing life within the community and relations between communities. In the broadest sense, these norms can be defined as politics, varying throughout history in accordance with humanity's transformations, with the primary purpose of creating the necessary harmony for peaceful coexistence. Any disruptive factor affecting this harmony, followed by the failure of politics to restore

the previous balance, leads to a violent manifestation of the struggle for survival. Thus, warfare emerged, which is nothing more than *"the continuation of politics by other means"* (Clausewitz, 2007, p. 28), characterised by *"the massacre of people who do not know each other, in favour of people who know each other but will not massacre each other"* (Citatopedia[®].ro, 2005, p. 1). With chameleon-like traits (Clausewitz, 2007, p. 30), the evolution and transformation of warfare are synchronised with that of human society, with each aspect of life being influenced by and, in turn, influencing this complex and violent phenomenon. Thus, in the past, the term 'war' strictly referred to military confrontation – the army being the only *"specialised organism for waging war"* (Duțu, Moștofleu, & Sarcinschi, 2003, p. 3) – while today we witness the use of this term in various fields, such as technological, informational, economic, energy etc., where the military component is small, often insignificant, or even absent.

As a result, most experts and dictionaries provide complex definitions that highlight the diversity of areas in which warfare can manifest (Cambridge Dictionary, 1999), (Merriam-Webster's Dictionary, 2011). Additionally, in an effort to develop a definition that encompasses all aspects and nuances resulting from technological advances or the spiritual transformations of society, as well as the challenges arising from these, new concepts have emerged, such as *"new type warfare"* (Kaldor, 2012, p. 1), *"fourth-generation warfare"* (4GW) (Echevarria, 2005, p. 1), *"non-linear warfare"* (Schnaufe, 2017, p. 20) or *"hybrid warfare"* (Hoffman, 2007, p. 28). This work focuses on defining and understanding the latter term, in general, and on *hybrid maritime warfare*, in particular.

Generalities

The complexity of military actions and the multitude of effects felt in increasingly many areas of human society, generated both in the preparation phase (modelling/competition) and in its execution, result in difficulties in formulating a comprehensive and widely accepted theory or definition of the new type of warfare facing humanity. Among the multitude of terms defining this new type of conflict, we will further analyse *hybrid warfare* in an attempt to identify a definition



ROMANIAN
MILITARY
THINKING

The complexity of military actions and the multitude of effects felt in increasingly many areas of human society, generated both in the preparation phase (modelling/competition) and in its execution, result in difficulties in formulating a comprehensive and widely accepted theory or definition of the new type of warfare facing humanity.



that covers the entire spectrum of actions and threats, whose effects have multilateral reverberations, with their central purpose being to create the most favourable conditions for conflict cessation negotiations.

At the introduction of the term hybrid warfare, Frank Hoffman defines it as *“warfare that incorporates a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion, and criminal disorder”* (Hoffman, 2007, p. 21). In the same idea of complexity in hybrid threats, they are defined as *“methods and activities that target an adversary’s vulnerabilities. Vulnerabilities may result from a confluence of factors, including historical memory, legislation, old practices, geopolitical factors, strong societal polarization, technological disadvantages, or ideological differentiations. If the interests and objectives of hybrid actions are not achieved, the situation can escalate into hybrid warfare, in which the role of the military and violence will significantly increase”* (Hybrid CoE Working, 2019, p. 11). Analysing these two definitions, we can conclude that the broad and varied range of methods used to exploit various vulnerabilities of an opposing entity to achieve objectives, as well as the imminence of armed conflict in the event that the effects of unconventional tactics do not converge towards the accomplishment of the entire action’s goal, highlights the particularly important role that the military instrument plays in maintaining the parameters of the security equation at the state, regional, and global levels.

The major role of the military component was emphasised at the NATO summit in 2014, held in Wales, by highlighting the fact that overt or covert actions carried out by military personnel, coordinated with paramilitary and civilian actions, are undertaken within an integrated design (North Atlantic Treaty Organization, 2014). From this, we can deduce that hybrid warfare tends to *borrow* elements such as action planning, analysis, and operational design, which are specific to conventional warfare. In response to these actions, a series of measures have been identified, such as *“improving strategic communication, developing exercise scenarios in light of hybrid threats, and enhancing coordination between NATO and other organizations, in accordance with relevant decisions, to improve information exchange, political*

consultations, and coordination among the armed forces of member countries” (Ib.).

The importance of hybrid warfare has not only been recognised and analysed by NATO member countries; these techniques and procedures have been successfully used by the Russian Federation in conflicts in Georgia and more recently with Ukraine. Heavily influenced by the conflicts in Chechnya, Russian military thinking has understood that the fusion of unconventional military tactics with informational warfare (IW) and psychological operations (PSYOps) is very challenging to counter. As a result, Moscow’s military leaders have used the conflicts in 2008, 2014, and 2022 to validate the theory that the coordinated, integrated, and synchronised engagement of conventional military force with irregular units can be used as an instrument of foreign policy, while demonstrating that, strategically, gains could be achieved with low long-term costs (Murphy & Schaub, *“Sea of Peace”* or *Sea of War – Russian Maritime Hybrid Warfare in the Baltic Sea, 2018*, pp. 2-3). It is easy to observe that in this case as well, hybrid warfare is perceived as a complex threat arising from the combination of military actions with those of other structures and entities, whose synergistic effects target not only the adversary’s military but also civilian society with the aim of destabilizing and dividing support for the war effort.

In the same idea, in the doctrine bearing his name, the Chief of the Russian General Staff, General Valery Gerasimov, defines hybrid warfare as a combination of *“military, technological, informational, diplomatic, economic, cultural factors, and other tactics involved in achieving strategic objectives”* (Islam, 2021, p. 1). From the enumeration of all the factors involved in the Gerasimov Doctrine, one could erroneously deduce that the military component’s weight is reduced. However, one of the most significant innovations introduced by the Russian general is that military actions are and will be crucial in achieving objectives, with the real challenge being the identification of optimal methods for involving military means, as they can no longer act independently of non-military ones, and strategic-level objectives cannot be achieved without the coordination of efforts between these two structures.

In the context of Russia’s approach to hybrid warfare and as a NATO member state, Romanian military thinking has also addressed this concept with the aim of fully understanding the challenges posed



In the doctrine bearing his name, the Chief of the Russian General Staff, General Valery Gerasimov, defines hybrid warfare as a combination of “military, technological, informational, diplomatic, economic, cultural factors, and other tactics involved in achieving strategic objectives”.

“Vulnerabilities may result from a confluence of factors, including historical memory, legislation, old practices, geopolitical factors, strong societal polarization, technological disadvantages, or ideological differentiations. If the interests and objectives of hybrid actions are not achieved, the situation can escalate into hybrid warfare, in which the role of the military and violence will significantly increase”.



by a complex and ambiguous security environment in which military leaders are forced to make decisions based on uncertain and often insufficient information. Consequently, according to some experts, hybrid warfare is *“the exploitation of a tandem of favourable and unfavourable situations by a potential adversary, by supporting and improving unfavourable situations until the success of a major socially impactful negative event”* (Roman, 2022, p. 83). Furthermore, the success of this negative event is defined as focusing *“not only on causing damage and exploiting opportunities but rather on destabilising society as a whole, creating ambiguity with the purpose of jeopardizing the counteraction to the effects of hybrid-type negative manifestations and, implicitly, the entire decision-making process”* (Roman, 2022, p. 83).

Hybrid warfare is “the exploitation of a tandem of favourable and unfavourable situations by a potential adversary, by supporting and improving unfavourable situations until the success of a major socially impactful negative event”.

In **conclusion**, regardless of how *hybrid warfare* is defined, there are no major conceptual differences stemming from the status of being a single state or a member of an alliance, or from belonging to the military or civilian system. Analysing the specialised literature, we can observe that the majority of definitions revolve around the idea of *gaining a significant advantage at the strategic, operational, or tactical level through coordinated actions of the state’s civilian and military authorities, along with the involvement of non-state actors*.

Furthermore, by encompassing nearly all aspects of societal life (Stanciu, 2016, pg. 13-15), hybrid actions have their effects felt across all domains specific to military actions, from the most recent ones such as space and cyber, to the traditional terrestrial, aerial, and maritime domains. The specifics of the latter will be analysed in the following sequence of this scientific endeavour.

The Specifics of Hybrid Maritime Threats

The low costs associated with maritime transport represent both an advantage and a disadvantage of the maritime environment. On one hand, the advantage arises from the understanding of the importance of maintaining freedom of navigation on the world’s seas and oceans, as manifested in the signing of numerous international conventions in which most states are signatory parties. On the other hand, jeopardizing maritime communication lines has had and will continue to have a major impact on a state’s economy, whether it has access to the global ocean or not.

The importance of safeguarding the maritime environment and the need to reduce its specific vulnerabilities, especially in the face of hybrid threats, constitute a significant item on the NATO and EU agendas. Thus, in the joint declaration from Warsaw on 8 July 2016, representatives of these organisations underscore the necessity of countering hybrid threats. One of the identified methods emphasizes expanding and adapting maritime cooperation, particularly for reducing the phenomenon of immigration, by promoting the resilience of member states in the eastern and southern flanks and through projects in various areas, with the common goal of strengthening maritime capacity (NATO, 2016).

Generating an adequate response to any type of threat requires, first and foremost, identifying that threat and how it can negatively impact one or more states. Therefore, when countering hybrid threats in the maritime environment, it is necessary to analyze it from the perspective of vulnerabilities that can be exploited. After studying the specialised literature, we have found that most hybrid actions focus on the ambiguity of provisions in international treaties and conventions, the cyber environment, surface or submarine means and installations, as well as the maritime transportation system.

The most exploited vulnerabilities stemming from the ambiguity of international treaties and conventions are related to the delimitation of territorial waters, contiguous zones, or exclusive economic zones, as well as the regulation of transit through straits. From the perspective of maritime means and installations, hybrid threats focus on undersea communication cables, the majority of which lack even basic protection, despite being responsible for over 97% of intercontinental communications traffic (Center for International Maritime Security, 2018). Maritime transportation can be significantly affected either by disrupting the functioning of technological systems on board vessels or by the operational status of port facilities and installations. The exploitation of vulnerabilities in the cyber environment, which is ubiquitous in society, is felt across all sectors of activity, whether related to the maritime environment or not.

Furthermore, the maritime space can be affected by hybrid actions, whether planned or not, carried out within the territory of a state far from its coastline. An example of this is the closure in 2007



ROMANIAN
MILITARY
THINKING

Most hybrid actions focus on the ambiguity of provisions in international treaties and conventions, the cyber environment, surface or submarine means and installations, as well as the maritime transportation system.



of the ferry line between the Estonian port of Sillamae and the Finnish port of Kotka due to the refusal of transit authorization through Russian territorial waters by the vessel Vironia. Most likely, the refusal by Russian authorities was prompted by the outrage of the Russian-speaking residents of the Finnish capital caused by the relocation of the bronze monument of the Soviet Soldier in Tallinn (Center for International Maritime Security, 2020). This action immediately led to increased discontent among the population and decreased trust in authorities, potentially resulting in negative effects on national security, which is one of the most frequently targeted objectives of hybrid actions.

The energy crisis, driven by the dependency on gas imports from the Russian Federation, has compelled EU member states to identify new sources of supply. In the absence of underwater pipelines for transporting petroleum products, the flow of liquefied natural gas (LNG) and other oil products depends on shipping vessels and onshore unloading facilities, with most of these being owned by commercial operators.

The energy crisis, driven by the dependency on gas imports from the Russian Federation, has compelled EU member states to identify new sources of supply. In the absence of underwater pipelines for transporting petroleum products, the flow of liquefied natural gas (LNG) and other oil products depends on shipping vessels and onshore unloading facilities, with most of these being owned by commercial operators. Additionally, the exploration of gas and oil in the eastern Mediterranean and their transshipment by sea are primarily the domain of private business enterprises. All of these factors increase the vulnerability of the energy supply chain, with hybrid threats focused on commercial entities engaged in exploring, extracting, and shipping these goods, either due to their sometimes-different interests from those of the state or because of a lack of readiness and understanding of the consequences of these actions on other aspects of society.

From the information presented, it is clear that, as in other specific cases, in the maritime domain, the main characteristic of hybrid threats is *diversification*, both in terms of the methods used and the results and effects achieved. Therefore, we believe that only through optimal and robust *resilience* can the effects of these threats be successfully countered. To increase the maritime domain's resilience to hybrid attacks, a first step is the realistic identification of vulnerabilities in this domain, with optimal solutions resulting from an analysis of responsible and decision-making factors.

Building resilience is closely linked to a more precise understanding of the causes that generate vulnerabilities. Maritime security,

instrumentalised migration, critical infrastructure, the economy, aviation and space (Hybrid COE, 2017), maritime transportation including port infrastructure, cyberspace, the energy system, including its dependent resources, communication systems, especially undersea communication cables, and geographic or territorial vulnerabilities (Center for International Maritime Security, 2018), are examples of *preferred targets* for hybrid threats. The multiple vulnerabilities in these areas stem from a multitude of factors, such as legislative ones, the inter- and intra-state interdependence of economic activities, territorial disputes, or frozen conflicts, among others.

Taking into account what has been presented, we can **conclude** that there is an increase in the share of hybrid threats in all areas of human society, and the maritime domain is no exception. Their main objective is the disorganisation, interruption, and delay of both cargo and passenger transport by water, as well as economic activities related to the exploitation of maritime resources. When efficiently coordinated, the effects of these actions are felt in the military spectrum, by diminishing the war effort, increasing dissatisfaction in society, and creating pressure on authorities to put an end to these costly actions.

Characterised by a low degree of predictability, hybrid actions themselves are difficult to counter. However, by raising awareness of the situation and conducting a judicious analysis of maritime objectives and the tactics used by state and non-state actors that may undertake such actions, it is possible to anticipate scenarios of using these actions and determine the best ways to enhance the resilience of the state, thus minimising the adverse consequences on national stability and sovereignty.

Regarding the increase of the resilience of the Romanian state against hybrid threats in the maritime domain, it is necessary, first and foremost, to identify vulnerabilities of any nature in the Black Sea, whose exploitation could generate one or more economic, military, or other advantages for a potential adversary or have the effect of reducing the state's defence capability.



There is an increase in the share of hybrid threats in all areas of human society, and the maritime domain is no exception. Their main objective is the disorganisation, interruption, and delay of both cargo and passenger transport by water, as well as economic activities related to the exploitation of maritime resources.



GEOGRAPHIC AND ECONOMIC VULNERABILITIES IN THE BLACK SEA REGION FROM THE PERSPECTIVE OF HYBRID THREATS

According to the United Nations Convention on the Law of the Sea from 10 December 1982 (United Nations – Oceans and Law of the Sea, 2022), Romania, as a country with access to the Black Sea, enjoys sovereign rights and exclusive economic control over internal maritime waters (IMW), territorial waters (TTW), the contiguous zone (CZ), and the exclusive economic zone (EEZ). However, these rights also come with certain obligations and responsibilities. Primarily, authorities have a duty to maintain freedom of navigation in these areas by appropriately marking navigational hazards, recommending safe routes for navigation, providing information and notices to mariners, and ensuring a satisfactory level of security so that economic activities can proceed optimally.

The expansion of the national territory and the state’s responsibility over the maritime domain not only brings benefits but also diversifies the risks and threats to the state’s security. Any disturbance in the maritime security situation immediately impacts maritime transport and underwater economic activities, causing cascading effects on all sectors of society. Furthermore, the high level of interconnectedness among states through instant global communications, coordinated and integrated financial systems and trade, increases the speed and distance of the propagation of these effects, with consequences extending beyond a single state’s borders. Among all these aspects, we will focus on the geographic and economic vulnerabilities that, when exploited through hybrid actions, can generate certain military or other advantages by affecting a state’s military power or authority.

Geographic Vulnerabilities in the Black Sea

The maritime space can be considered both an advantage and a source of challenges for nations with a coastline. The advantages stem from the opportunity to exploit significant economic resources in this space, establish commercial routes with distant states, or develop tourism services. However, the challenges are driven by technological advancements in resource exploitation and, more importantly, the very high costs of maintaining an optimal level of security for conducting

economic activities. From this perspective, the Romanian Naval Forces, as a branch of the armed forces responsible for ensuring maritime safety (Legea nr. 346/2006 privind organizarea și funcționarea Ministerului Apărării Naționale, 2006, p. art. 5, 28), face several challenges due to their Maritime Responsibility Area of 29,851 square kilometers in the Black Sea (which includes the Internal Maritime Waters – AMI, Territorial Waters – TTW, Contiguous Zone – ZC, and Exclusive Economic Zone – ZEE).

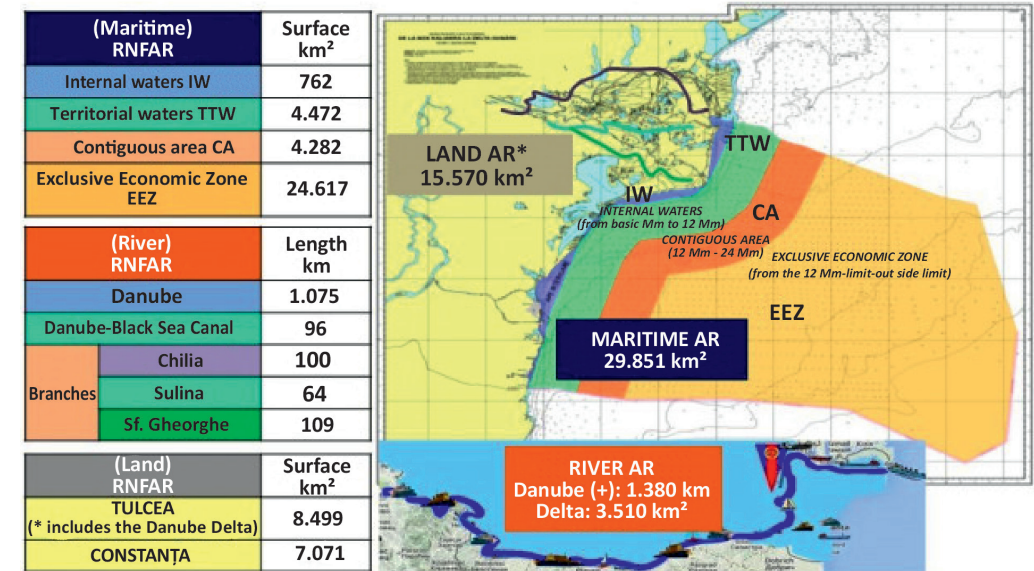


Figure 1: The responsibility area of the Romanian Naval Forces (Forțele Navale Române, 2022)

Moreover, the relatively small surface area of the Black Sea compared to the world’s oceans and its status as a semi-closed sea open up new opportunities for a potential adversary to exploit the vulnerabilities of any coastal state. For Romania, a significant vulnerability is generated by the approximately 24,617 square kilometres of the Exclusive Economic Zone, in relation to the relatively low number of vessels in the inventory of the Romanian Naval Forces. Since one of the main missions of the Romanian Naval Forces includes defending the country’s interests, ensuring sovereignty and safety in the Black Sea, safeguarding freedom of navigation in the responsibility area, as well as protecting critical infrastructure elements along the coastline, territorial waters, and Romania’s Exclusive Economic

The expansion of the national territory and the state’s responsibility over the maritime domain not only brings benefits but also diversifies the risks and threats to the state’s security. Any disturbance in the maritime security situation immediately impacts maritime transport and underwater economic activities, causing cascading effects on all sectors of society.



Zone (Matache-Zaharia, 2014, pp. 154-159), we can conclude that maintaining an optimal level of safety in Romania's maritime area requires significant human, material, and financial efforts.

Through the Port of Constanța, our country has access to both the longest network of inland waterway transport in Europe, represented by the Rhine-Main-Danube transport corridor, connecting the North Sea to the Black Sea, and a rich Exclusive Economic Zone with various resources, especially hydrocarbons (lb.). One possible solution for achieving the common goal of deterring any hostile action, regardless of its nature or character, towards national security from the maritime perspective is the cooperation between naval forces and aviation.

Through the Port of Constanța, our country has access to both the longest network of inland waterway transport in Europe, represented by the Rhine-Main-Danube transport corridor, connecting the North Sea to the Black Sea, and a rich Exclusive Economic Zone with various resources, especially hydrocarbons.

Furthermore, there is a rapid increase in the utilisation of space and satellites for communication, monitoring, and early warning services, where the expansion of private services also aims to enhance maritime national resilience. Internationally, the rapidly evolving competition in the military use of outer space has generated various issues, from legislative regulation to moral dilemmas, through the formulation of accusations, with or without concrete evidence, that some states employ space for purposes other than those declared (Hybrid COE, 2017). From a security standpoint, the purpose of any state's actions, represented in the maritime environment by its naval forces, is to explore vulnerabilities related to hybrid threats and to pave the way for identifying the best solutions and recommendations to enhance resilience, the main pillar in reducing or nullifying the effects of maritime hybrid threats and actions.

In **conclusion**, when analysing the hybrid threats posed by a potential adversary, it is necessary to understand that the optimal strategy for countering them, in most cases, involves deterring or delaying their hostile actions. To achieve this goal, it is essential for the Romanian Naval Forces to make their presence felt in the area of interest, simultaneously conducting a promotional campaign through mass media and social media to showcase exercises and missions carried out in the Black Sea.

However, the mere surface presence of naval vessels does not entirely eliminate the risks and does not necessarily deter or nullify the opponent's actions, as observing them for a period of time

can reveal vulnerabilities that can be exploited. Consequently, it is crucial to maintain and enhance naval capabilities that can operate without being observed by the adversary. From our perspective, equipping the Romanian Naval Forces with submarine capabilities could be a priority for military leadership, with the task of convincing the political authorities about the importance, necessity, and, most importantly, the benefits to Romanian society of ensuring an optimal security environment in the Black Sea.

Economic Vulnerabilities in the Black Sea

Since the economy is vital for the survival and development of every country, it also has numerous vulnerabilities that adversaries can exploit. In order to maintain a conducive environment for economic activities, optimal solutions for increasing resilience can be identified by assessing vulnerabilities from various perspectives, including the military and economic ones (Hybrid COE, 2017). Competition, as a form of human nature, is present in the economic domain and can be approached as a factor with a pronounced hybrid character that is unfolding on a global scale, with the maritime environment serving as the common thread that interconnects the world's nations.

From an economic perspective, in the maritime environment, we are particularly referring to waterborne transportation, which is one of the key contributors to a state's development. Commercial ships and port infrastructures are essential for sustaining a state's growth. However, they are vulnerable to hybrid threats in the form of sabotage, falsification of navigation data, or cyberattacks on supply chain information systems. These actions immediately impact maritime traffic, resulting in the loss or disruption of the supply chain for goods or the denial or hindrance of access to critical port facilities (Kotman). Equally noteworthy are the damages inflicted on the maritime environment, characterised by the enormous costs of mitigating the harmful effects on marine fauna and flora.

Closely related to the economic aspects at sea is the energy sector, where achieving energy independence is a goal most countries aspire to reach. The need for diversification of energy supply has led to the increased importance of natural gas exploitation and transportation.



ROMANIAN
MILITARY
THINKING

In order to maintain a conducive environment for economic activities, optimal solutions for increasing resilience can be identified by assessing vulnerabilities from various perspectives, including the military and economic ones.



Thus, on the waterways, in addition to the transportation of general cargo, there is a rapid increase in the traffic of vessels specifically designed for the transportation of liquefied natural gas (LNG), as well as a rising trend in onshore loading/unloading facilities (Ib.).

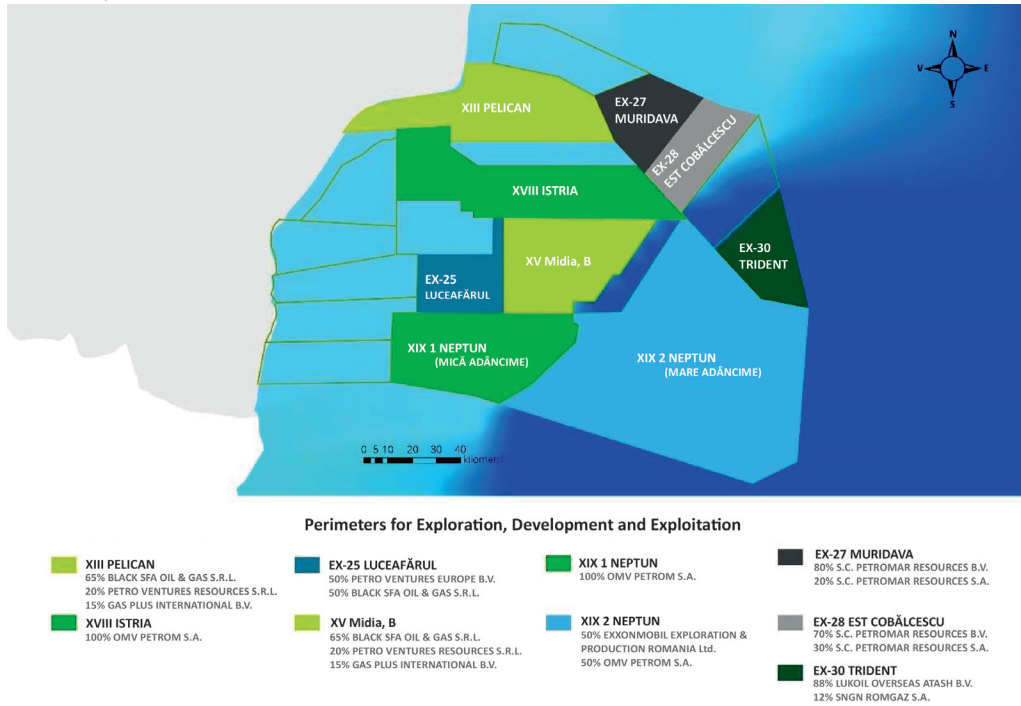


Figure 2: The Romanian offshore area (Deloitte Touche Tohmatsu Limited, 2018, p. 12)

Romania's Exclusive Economic Zone is rich in hydrocarbons and various resources, and the exploitation of these resources is a priority for the central authorities of the state. To achieve this objective, the state relies on private economic operators, whose origins can be found on any meridian. This fact represents a vulnerability in the economic environment specific to the maritime space since there is not always a convergence of interests between these operators and those of the state. Thus, a specialized actor in hybrid actions can exploit these vulnerabilities for their own benefit and create a security breach, the effects of which can be felt in many aspects of Romanian society over time.



The range of hybrid actions that can be directed towards the economic sector in general and the economic activities specific to the maritime environment varies, from using migration as a hybrid threat instrument in the context of humanitarian law (Hybrid COE, 2017), to actions like the destruction of submarine gas transport pipelines, as was the case with the explosions at the Nord Stream gas pipeline on 26 September 2022 (Şancu, 2023). These incidents, in addition to causing material damage, also registered effects on public opinion on various issues.

In this broad palette of hybrid actions, special attention should be given to actions in the cyber environment. The increasing dependence on the internet and the degree of digitization and automation in various systems and activities mean that the effects in the cyber domain can propagate cascade into systems, organisations, or activities that initially seem to have no connection with those targeted by a hybrid actor. From navigation systems to port information systems, maritime activities, whether commercial or related to the military, rely more than ever on cyber capabilities (Kotman). Being interdependent, all these systems are vulnerable to cyber-attacks by hybrid actors and criminal organisations. Furthermore, the perspective of the development and widespread use of unmanned ships generates obvious major risks when viewed through the lens of maritime hybrid threats. One potential scenario involves a cyber-hacked unmanned ship being transformed into a weapon.

As a result of this analysis, we can **conclude** that hybrid warfare is not a clearly new phenomenon, and the aggressor usually uses gray zones to complicate the decision-making regarding the legality of their actions in conflict situations. From the perspective of other states, the aggressor makes it difficult to take decisive measures in response.

The gray zone in hybrid warfare can be understood as a space of limited and ambiguous military action, in which the aggressor creates enough ambiguity to achieve their strategic objectives without engaging in open warfare. In other words, it is not entirely clear to what extent the law of the sea applies in conflicts with a pronounced hybrid character. Intertwined with the question of whether maritime law or the legal framework for the application of the law should be

The increasing dependence on the internet and the degree of digitization and automation in various systems and activities mean that the effects in the cyber domain can propagate cascade into systems, organisations, or activities that initially seem to have no connection with those targeted by a hybrid actor.



applied in so-called gray zones to assess the legality of the use of force or direct coercion by the coastal state at sea, these actions can affect the smooth conduct of economic activities in the maritime environment. The implications of this disruption are felt in all areas, including national security.

CONCLUSIONS

While not guaranteeing complete success, a series of measures, such as adopting a robust common communications strategy to counter Russian information operations or reducing energy dependence on Russia, can be part of a more comprehensive plan to mitigate the effects of its hybrid actions. Furthermore, the fact that after the annexation of Crimea, NATO and the Russian Federation share a common border in the Black Sea emphasises the importance of the maritime domain. Therefore, the critical role of maritime and submarine infrastructure can be demonstrated by highlighting the significance of using the sea for collecting, analysing, and disseminating information, with a focus on hybrid threats. The ultimate goal is to increase the resilience of a state and, by extension, the alliance itself.

Regarding responsibilities in the maritime environment, the ability to control, maintain, and protect territorial waters, the contiguous zone, and the exclusive economic zone is a key aspect of governance. In Romania, this is reflected in the National Defence Strategy and all subsequent normative acts. Consequently, military normative acts translate this strategic objective into the central tasks of the Naval Forces and the Coast Guard.

Romania's maritime interests are linked to military defense projects aimed at ensuring an optimal environment for the development and maintenance of energy independence, as well as ensuring freedom of navigation. It is also crucial to understand the essential role of interconnected critical services that fuel and enhance national economic development. Modern critical infrastructure is a preferred target in the view of actors generating hybrid threats, whether state or non-state.

Intact and functional critical infrastructure elements in the maritime environment are vital for the well-being of society as a whole.

As a result, one of the main concerns of decision-making bodies at the highest level should be focused on reducing the geographical and economic vulnerabilities of the country in the Black Sea by acquiring the necessary means for the Romanian Naval Forces to anticipate and counteract any action, whether hybrid or not, by a potential adversary.

Building resilience is essential when it comes to countering hybrid threats. A good understanding of the underlying causes of exploitable vulnerabilities is necessary. Since hybrid threats target multiple sectors of society in complex ways, resilience must be approached sector by sector. However, overall societal resilience must also be implemented.

BIBLIOGRAPHY:

1. Cambridge Dictionary. (1999). *Cambridge Dictionary*, <https://dictionary.cambridge.org/dictionary/english/war>, retrieved on 19 November 2022.
2. Center for International Maritime Security. (2018). *Countering Hybrid Threats in the Maritime Environment*, <https://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/>, retrieved on 12 April 2022.
3. Center for International Maritime Security. (2020). *Implications of Hybrid Warfare for the Order of the Oceans*, <https://cimsec.org/implications-of-hybrid-warfare-for-the-order-of-the-oceans/>, retrieved on 12 April 2022.
4. Citatepedia®.ro. (2005). *Citate, aforisme, proverbe, replici, versuri...*, <http://www.citatepedia.ro/index.php?id=10244>, retrieved on 19 November 2022.
5. Clausewitz, C. v. (2007). *On War*. Oxford: Oxford University Press.
6. Deloitte Touche Tohmatsu Limited. (2018). *Deloitte Report: Investments in Black Sea Oil and Gas Sector Will Bring Over 26 Billion USD to the State Budget*, <https://www2.deloitte.com/content/dam/Deloitte/ro/Documents/ImpRepOffshoreProjects-ENG.PDF>, retrieved on 12 May 2023.
7. Duțu, P., Moștofleu, C., Sarcinschi, A. (2003). *Profesionalizarea Armatei României*. București: Centrul de Studii Strategice de Apărare și Securitate.
8. Echevarria, A. (2005). *Fourth-Generation War and Other Myths*. U. S. Government, Ed. Carlisle: Carlisle: Strategic Studies Institute.
9. Forțele Navale Române. (2022). *Forțele Navale Române monitorizează, sistematic, spațiul naval românesc*, <https://www.navy.ro/eveniment.php?id=1511>, retrieved on 13 February 2023.
10. Forțele Navale Române. (2023). *Forțele Navale Române – Organizare, Forțele Navale Române*, <https://www.navy.ro/despre/organizare/organizare.php>, retrieved on 10 February 2023.



Intact and functional critical infrastructure elements in the maritime environment are vital for the well-being of society as a whole. As a result, one of the main concerns of decision-making bodies at the highest level should be focused on reducing the geographical and economic vulnerabilities of the country in the Black Sea by acquiring the necessary means for the Romanian Naval Forces to anticipate and counteract any action, whether hybrid or not, by a potential adversary.

Regarding responsibilities in the maritime environment, the ability to control, maintain, and protect territorial waters, the contiguous zone, and the exclusive economic zone is a key aspect of governance. In Romania, this is reflected in the National Defence Strategy and all subsequent normative acts. Consequently, military normative acts translate this strategic objective into the central tasks of the Naval Forces and the Coast Guard.



11. Hoffman, F. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, Virginia: Potomac Institute for Policy Studies.
12. Hybrid COE. (2017). *COI Vulnerabilities and Resilience*, <https://www.hybridcoe.fi/coi-vulnerabilities-and-resilience/>, retrieved on 18 December 2022.
13. Hybrid CoE Working. (2019). *Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans*. Helsinki: Hybrid CoE.
14. Islam, A. (2021). *The Valery Gerasimov Doctrine*. *BIPSS Commentary*, 1-6.
15. Kaldor, M. (2012). *New and Old Wars. Organised Violence in a Global Era*. Boston, Malden, MA 02148, USA: Polity Press.
16. Kotman, T. (f.a.). *Maritime Hybrid Threat*, from Maritime Security Center of Excellence, <https://www.marseccoe.org/wp-content/uploads/2021/08/Maritime-Hybrid-Threat.pdf>, retrieved on 14 September 2023.
17. Matache-Zaharia, S.-A. (2014). *Buletinul Universității Naționale de Apărare "Carol I"*, *Buletinul Universității Naționale de Apărare "Carol I"*, file:///E:/Download/%23%23common.file.namingPattern%23%23.pdf, 10 February 2023.
18. Merriam-Webster's Dictionary. (2011). *Merriam-Webster's Dictionary*, <https://www.merriam-webster.com/dictionary/war>, retrieved on 19 November 2022.
19. Murphy, M., Schaub, G. (2018). *"Sea of Peace" or Sea of War - Russian Maritime Hybrid Warfare in the Baltic Sea*. *Naval War College Review*, 71(2), 1-26, <https://digital-commons.usnwc.edu/nwc-review/vol71/iss2/9>, retrieved on 22 August 2023.
20. Murphy, M., Hoffman, F., Schaub, G. (2016). *Warfare and the Baltic Sea Region*. Copenhagen: Center for military studies, University of Copenhagen.
21. NATO. (2016). *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en, retrieved on 12 April 2022.
22. North Atlantic Treaty Organization. (2014). *Wales Summit Declaration*, https://www.nato.int/cps/us/natohq/official_texts_112964.htm, retrieved on 19 November 2022.
23. Parlamentul României. (2006). *Legea nr. 346/2006 privind organizarea și funcționarea Ministerului Apărării Naționale*. *Monitorul Oficial, Partea I nr. 867 din 2 noiembrie 2017*. București: Monitorul Oficial, Part I nr. 867 of 2 November 2017.
24. Roman, D. (2022). *Hybrid Warfare or the "Black Swan" in the New Contemporary Societal Context*. In *Romanian Military Thinking*, nr. 2, pp. 74-85. doi:10.55535/RMT.2022.2

25. Schnaufe, T. (2017). *Redefining Hybrid Warfare: Russia's Non-linear War against the West*. *Journal of Strategic Security*, 10(1), 17-31. doi:<http://doi.org/10.5038/1944-0472.10.1.1538>.
26. Stanciu, C. (2016). *Viitorul conflictualității – Operații asimetrice și hibride*. București: Editura Universității Naționale de Apărare "Carol I".
27. Șancu, S. (2023, 03 08). *Europa Liberă România*, *Explozia Nord Stream. Complot pro-ucrainean sau operațiune sub steag fals marca Kremlin?*, <https://romania.europalibera.org/a/explozie-nord-stream/32308462.html>, retrieved on 12 August 2023.
28. United Nations Oceans and Law of the Sea. (2022). *Division for Ocean Affairs and the Law of the Sea*, https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm, retrieved on 1 August 2023.

