NEW STRATEGY CENTER

www.newstrategycenter.ro/en

Protecting Critical Maritime Infrastructure in the Black Sea

Sergiu MITRESCU

Program Director, New Strategy Center

Author: Sergiu Mitrescu, Program Director, New Strategy Center

Sergiu Mitrescu is the Program DIrector of New Strategy Center. His research revolves around the intersection of maritime security and hybrid threats with a particular focus on critical maritime infrastructure.

Editor: George Scutaru, CEO, New Strategy Center, former national security advisor to the Romanian President

About New Strategy Center

New Strategy Center is a Romanian think tank specializing in foreign, defence and security policy, a non-partisan, non-governmental organisation. New Strategy Center operates at three main levels: providing analytical inputs and expert advice to decision-makers; holding regular debates, both inhouse and public, on subjects of topical interest; expanding external outreach through partnerships with similar institutions or organisations all over the world, joint policy papers and international conferences. The Balkans and the Black Sea space are priority areas of interest for New Strategy Center.

Disclaimer: This text contains the personal opinions and perspective of the authors and does not necessarily reflect the views of the New Strategy Center.

Cover: Offshore oil and gas platform, source: shutterstock; Broken submarine cable, source: shutterstock

Descrierea CIP a Bibliotecii Naţionale a României
MITRESCU, SERGIU
Protecting critical maritime infrastructure in the Black Sea / Sergiu Mitrescu. - Bucureşti : New Strategy Center, 2025
ISBN 978-606-95860-2-0

Sergiu MITRESCU

Protecting Critical Maritime Infrastructure in the Black Sea

New Strategy Center
2025

Protecting Critical Maritime Infrastructure in the Black Sea

Introduction

Critical maritime infrastructure (CMI) serves as a cornerstone of modern global interconnectedness, underpinning the movement of energy, goods, and information. These infrastructures, including undersea data cables, offshore oil and gas platforms, ports, and wind farms, are not only vital to economic stability and societal functioning but also critical to national and regional security. The rising importance of offshore areas in global geopolitics, driven by technological advances and resource scarcity, has brought their vulnerabilities into sharp focus. Recent high-profile incidents in the Baltic Sea have underscored the susceptibility of maritime infrastructures to hybrid threats.

Hybrid threats, characterized by a combination of conventional and unconventional tactics, exploit systemic vulnerabilities and operate below the threshold of open conflict. These threats are particularly potent in the maritime domain, where legal frameworks are often fragmented, and monitoring vast and remote areas poses significant challenges. In this environment, critical infrastructure becomes a lucrative target for adversaries seeking to disrupt vital services, destabilize political systems, and exert geopolitical leverage. Such actions have profound implications for security, as they expose the fragility of essential systems and challenge the resilience of nations and alliances.

The Black Sea region represents a focal point of maritime insecurity, serving as a microcosm of the challenges faced by CMI globally. This region, strategically significant for its energy resources, trade routes, and geopolitical tensions, has witnessed a marked escalation in hybrid threats. Russia's annexation of Crimea in 2014 fundamentally altered the regional security landscape, transforming the Black Sea into a contested arena for power projection and conflict. Russia's New Generation Warfare (NGW) tactics, which encompass cyberattacks, information warfare, and physical sabotage.

This study investigates the intersection of hybrid threats and CMI in the Black Sea, focusing on the material and ideational dimensions of infrastructure, the criticality of maritime assets, and the operational complexities posed by hybrid tactics. By addressing the vulnerabilities and lessons of CMI in the Black Sea, the study aims to provide actionable insights for policymakers and stakeholders to strengthen resilience in contested maritime regions.

Hybrid Threats

Hybrid threats represent a complex and evolving challenge in contemporary international relations, particularly in the maritime domain. These threats blend conventional military tactics with unconventional methods such as cyberattacks, disinformation campaigns, economic coercion, and sabotage. The ambiguity inherent in hybrid operations makes them particularly effective, as they operate below the threshold of conventional war, complicating attribution and response.

The term was coined in 2007[1] and came to dominate public debate following Russia's annexation of Crimea in 2014, which highlighted a sophisticated blend of strategic communication, covert military actions, and non-military measures aimed at destabilizing Ukraine. While-hybrid warfare has historical antecedents, including Soviet-era "active measures" and earlier forms of irregular warfare, its modern iterations leverage technological advancements and exploit systemic vulnerabilities across multiple domains.

A defining characteristic of hybrid threats is their reliance on ambiguity. By blurring the lines between military and civilian actions, peace and conflict, hybrid tactics challenge existing legal and normative frameworks. This ambiguity complicates the ability of states and international organizations to respond effectively, as it often remains unclear whether an incident constitutes an act of war, a criminal act, or a routine disruption. In the maritime domain, this ambiguity is heightened by the vastness and remoteness of oceanic spaces, where monitoring and enforcement are inherently challenging.

Russia's New Generation Warfare (NGW) serves as a paradigmatic example of hybrid threats in action. NGW tactics, as articulated in Russian military doctrine,

[1] Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid Wars (Arlington, VA: Potomac Institute for Policy Studies, 2007)

emphasize the use of non-military means to achieve strategic objectives. These tactics include cyberattacks on critical infrastructure, disinformation campaigns aimed at undermining public confidence, and the use of proxies and covert operatives to create instability. In the maritime context, these tactics have been directed at critical infrastructures such as undersea cables, offshore platforms, and shipping routes, often with significant geopolitical implications. Russia's New Generation Warfare (NGW) doctrine provides a comprehensive framework for hybrid threats, relying on a blend of kinetic operations, cyberattacks, disinformation campaigns, economic coercion, and legal maneuvers to achieve strategic objectives. Unlike conventional military engagements, NGW emphasizes ambiguity and plausible deniability, ensuring that adversarial actions fall below the threshold of open conflict. In the maritime domain, these tactics are particularly effective due to the fragmented legal frameworks governing international waters and the difficulties associated with surveillance and enforcement .

A key element of NGW is lawfare, whereby Russia leverages legal ambiguities to justify aggressive maritime activities. Since 2014, Russia has utilized exclusion zones and naval exercises as a pretext for restricting access to strategic maritime corridors. The declaration of extensive "temporary danger areas" in the Black Sea during military drills disrupts commercial shipping, raises insurance costs, and erodes the security environment for regional actors like Romania, Ukraine, and Bulgaria. This practice, coupled with aggressive patrols by the Black Sea Fleet, allows Russia to assert *de facto* control over contested maritime spaces without direct military engagement.

Moreover, Russia employs proxy actors and covert operatives to carry out acts of maritime sabotage. Intelligence reports suggest that hybrid operatives have conducted undersea cable tampering and unauthorized surveillance of offshore platforms, further highlighting the covert dimensions of NGW. By targeting commercial infrastructure, Russia can exert pressure on NATO allies while maintaining plausible deniability. These actions underscore the systemic vulnerabilities of CMI in the Black Sea, particularly in contested waters near Crimea and Romania's Exclusive Economic Zone (EEZ)

The Neptune Deep gas extraction project, situated in Romania's Exclusive Economic Zone (EEZ), exemplifies the strategic importance and vulnerability of CMI in the

Black Sea. This project is not only a critical component of Romania's energy strategy but also a symbol of its regional ambitions and resilience against Russian influence. The project is transformative in the sense that it can turn Romania into a net energy exporter, which in the regional context can satisfy the needs of energy countries with profound geopolitical implications.[2]

The project will operate at over 160km from the shoreline close to the extremity of Romania's EEZ and will be operated remotely through underwater energy and data infrastructure, a level of technological complexity which makes it vulnerable to hypothetical hybrid attacks.

The Black Sea has emerged as a key theater for the operationalization of hybrid threats. Since the annexation of Crimea, Russia has deployed a range of hybrid tactics to assert control over the region. For example, the Russian Black Sea Fleet has engaged in aggressive lawfare, declaring extensive military exercises that effectively block access to critical maritime zones. These actions disrupt freedom of navigation, create uncertainty for commercial shipping, and erode the principles of international law.

In 2022, Russian warships sailed in the proximity of Ana platform, Romania's most recent offshore addition.[3] The Ukrainian asymmetric successes in the Battle for the Black Sea contributed to the prevention of such aggressive actions by the Russian Federation which are likely to resume one the hostilities end and the Black Sea Fleet can return to its Sevastopol naval base.

---

[2] George Scutaru and Peter Watkins, Security Challenges in the Black Sea: NATO, the Wider Region, and the Global Order – Pledging for a Free and Open Black Sea (New Strategy Center, 2023).

[3] "Razboiul Rusiei împotriva Ucrainei: Nave rusești, dar și o mină, s-au apropiat periculos de cea mai nouă platformă petrolieră românească din Marea Neagră," Profit.ro, January 23, 2024, https://www.profit.ro/povesti-cu-profit/energie/video-foto-razboiul-rusiei-impotriva-ucrainei-nave-rusesti-dar-si-o-mina-s-au-apropiat-periculos-de-cea-mai-noua-platforma-petroliera-romaneasca-din-marea-neagra-21047639.

June 2022: Russian Ships near Romanian Gas Platform "Ana"

In 2023 a Russian SU-27 shut down an American MQ-9 Reaper drone over the Black Sea[4] while in the same year a SU-35 intercepting Polish FRONTEX plane over the Black Sea lead to temporary pause of the agency's operations[5].

The use of Maritime Autonomous Vehicles (MAVs) and Unmanned Aerial Vehicles (UAVs) has further expanded the toolkit of hybrid warfare in the maritime domain. MAVs and UAVs are increasingly deployed for surveillance, intelligence gathering, and sabotage, often with plausible deniability. During the conflict in Ukraine, Russia has utilized these technologies to disrupt maritime operations and target critical infrastructure. Their deployment underscores the adaptability of hybrid threats, as adversaries leverage emerging technologies to exploit vulnerabilities in maritime security.

MAVs, on the other hand, represent an emerging threat in hybrid maritime operations. These autonomous or semi-autonomous underwater vehicles can be deployed to sabotage undersea cables, conduct reconnaissance on offshore infrastructure, and interfere with military sonar operations. Their ability to operate undetected in deep waters makes them an ideal tool for covert actions targeting CMI.

---

[4] Natasha Bertrand, Oren Liebermann, and Haley Britzky, "Russian Fighter Jet Forces Down US Drone Over Black Sea After Intercept," CNN, March 14, 2023,https://edition.cnn.com/2023/03/14/politics/us-drone-russian-jet-black-sea/index.html.

[5] "Russia Intercepts Polish Jet Over Black Sea in 'Aggressive and Dangerous' Maneuver, Warsaw Says," Radio Free Europe/Radio Liberty (RFE/RL), May 7, 2023,https://www.rferl.org/a/russia-intercepts-polish-jet-/32400434.html.

Hybrid threats also extend to the economic and psychological dimensions of conflict. The sabotage of the NordStream pipelines, for example, disrupted energy flows to Europe, causing economic turmoil and political tension. Beyond the immediate physical damage, such incidents signal the fragility of critical infrastructure and instill fear and uncertainty among affected populations. This psychological dimension is a key component of hybrid tactics, as it seeks to undermine public confidence and weaken societal resilience.

The vulnerability of critical maritime infrastructure (CMI) in the Black Sea is not theoretical but has been demonstrated through real-world incidents that exemplify the breadth and severity of hybrid threats. The Nord Stream pipeline sabotage in 2022 provided a stark illustration of how maritime energy infrastructure can be directly targeted to create geopolitical instability. While attribution remains debated, the attack underscored how undersea energy networks are susceptible to both kinetic and covert operations. A similar case emerged with the Balticonnector gas pipeline disruption, which highlighted the challenges of securing maritime infrastructure across international waters.

In the Black Sea, the threat is even more acute. GPS jamming and spoofing incidents have been reported with increasing frequency, affecting both civilian and military navigation. Russian electronic warfare capabilities, particularly from installations in Crimea, have disrupted the navigation of vessels transiting the region, rendering Automated Identification Systems (AIS) unreliable and raising risks for commercial and naval operations.[6] This tactic aligns with a broader pattern of electronic interference, where cyber operations complement physical disruptions.

The impact of hybrid threats on critical maritime infrastructure (CMI) is profound. These threats target both the material and ideational dimensions of infrastructure. Materially, they disrupt the physical functioning of systems, such as the flow of energy or data. Ideationally, they undermine the symbolic and strategic value of infrastructure, eroding trust in national security frameworks and international norms. For example, the disruption of undersea cables not only hampers communication but also highlights the vulnerability of essential systems to adversarial actions.

[6] George Scutaru et al., The Battle for the Black Sea Is Not Over (New Strategy Center, 2024).

Legal considerations

Addressing hybrid threats requires a comprehensive and multidimensional approach. Existing legal and regulatory frameworks, such as the United Nations Convention on the Law of the Sea (UNCLOS), are often inadequate to address the complexities of hybrid operations. The ambiguity of hybrid tactics exploits gaps in these frameworks, highlighting the need for their reform and adaptation to contemporary challenges. Moreover, the integration of technological solutions, such as advanced surveillance systems and cyber defenses, is essential to enhancing the resilience of maritime infrastructure.

The protection of critical maritime infrastructure (CMI) is heavily influenced by the existing international legal frameworks that govern maritime activities, chief among them the United Nations Convention on the Law of the Sea (UNCLOS). While UNCLOS provides a comprehensive legal basis for defining maritime zones, resource rights, and navigation freedoms, it was drafted before the emergence of hybrid threats and therefore lacks the necessary provisions to address the complexities of modern security challenges. This gap has left states vulnerable to threats that exploit the ambiguity and limitations inherent in current governance frameworks.

UNCLOS establishes the legal parameters for maritime zones, including territorial seas, exclusive economic zones (EEZs) and the high seas along with guidelines for resource exploitation and environmental protection. However, its scope does not adequately account for the non-traditional and covert nature of hybrid threats. For example, hybrid operations, such as cyberattacks on offshore platforms or the use of Maritime Autonomous Vehicles (MAVs) for surveillance and sabotage, operate in a legal grey area where attribution and enforcement remain unclear.

Changes in de facto EEZ delimitations after the 2014 annexation of Crimea

One major limitation of UNCLOS lies in its enforcement mechanisms. While the convention grants coastal states jurisdiction over their territorial seas and certain rights within their EEZs, it does not provide clear guidelines for addressing non-state actors or state-sponsored hybrid operations that remain below the threshold of open conflict. This ambiguity is often exploited by adversaries to carry out covert actions, such as interfering with undersea cables or deploying MAVs to monitor or disrupt critical infrastructure.

Another significant challenge is the lack of legal clarity regarding the militarization of offshore zones. UNCLOS permits states to conduct military activities on the high seas, but it does not address the use of hybrid tactics, such as the deployment of armed drones or covert sabotage missions, within or near the EEZs of other states. This lack of specificity has created jurisdictional ambiguities, as seen in the Black Sea, where Russia's actions in contested waters often blur the line between legitimate military exercises and unlawful coercion.

The growing use of lawfare—where legal ambiguities are exploited to advance strategic objectives—further complicates the application of UNCLOS. For example, Russia's declaration of extensive exclusion zones during naval exercises disrupts commercial shipping and energy production in the Black Sea, undermining the rights of neighboring states. The practices are in accordance with international law but against the spirit of the law, with Russia taking advantage of provisions which rely on countries operating in goot faith. The blocking of perimeters for military exercises is

often justified under the pretext of national security, exposing the weaknesses of current legal frameworks in addressing hybrid threats that operate within these legal loopholes.

Jurisdictional Disputes in the Black Sea

The Black Sea exemplifies the complexities of jurisdictional disputes and their implications for maritime security. Following the annexation of Crimea in 2014, Russia claimed jurisdiction over significant portions of the Black Sea, including maritime zones that were previously under Ukrainian control. This *de facto* situation has had severe implications for international law leading to skirmishes such as in 2018, multiple Russian jets harassaed the HMS Duncan British destroyer sailing in the vicinity of Crimea's coast.[7] In 2021 a similar incident occurred involving HMS Defender HMS Defender, which was sailing from Odesa to Batumi via Crimea's territorial waters which sparking Russian protests in spite of its illegal claim.[8]

Flight Information Regions[9]

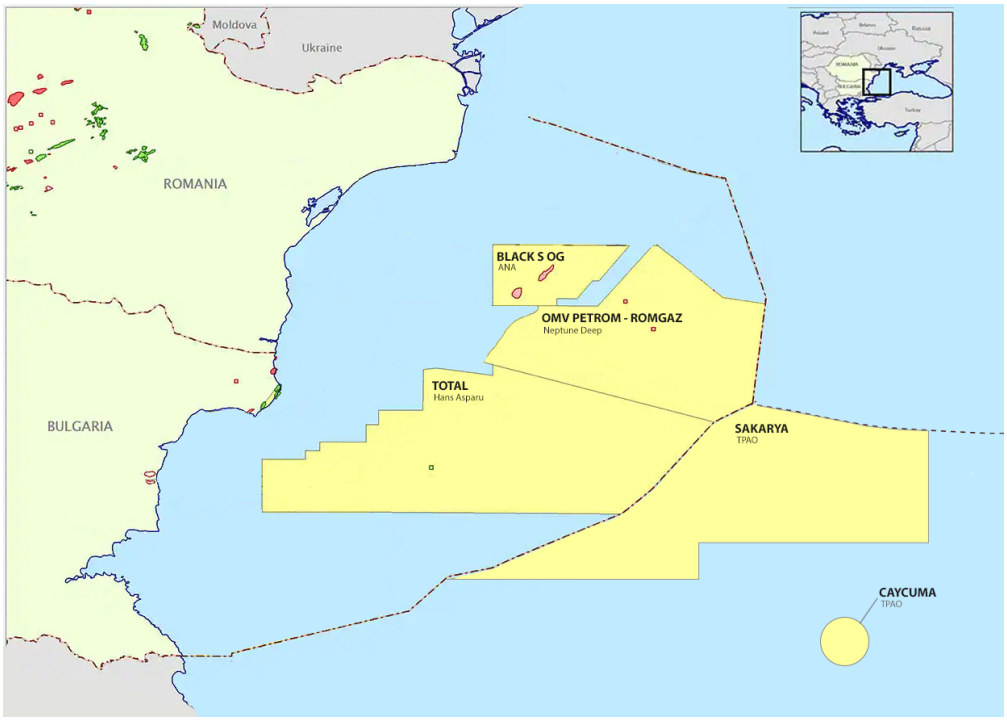
[7] Ryan Pickrell, "17 Russian Jets Buzzed a British Destroyer in the Black Sea," Business Insider, November 2, 2018,https://www.businessinsider.com/17-russian-jets-buzzed-a-british-destroyer-in-the-black-sea-2018-11.

[8] Mark Temnycky, "British Warship Challenges Russian Claims to Crimea," *Atlantic Council*, June 25, 2021, https://www.atlanticcouncil.org/blogs/ukrainealert/british-warship-challenges-russian-claims-to-crimea/.

[9] Eurocontrol. Flight Information Region (FIR/UIR) Charts 2024. Eurocontrol, 2024. https://www.eurocontrol.int/publication/flight-information-region-firuir-charts-2024

As well as absurd situations where the Simferopol Flight Information Region (UKVFV) flight area in over Crimea, parts of Southern Ukraine and the Western Black Sea including parts of Romania's and Bulgaria's EEZs is *de facto* administered by the Russian Federation[10] which has facilitated international air traffick until the onset of the 2022 full scale invasion.

For instance, offshore energy projects such as Romania's Neptune Deep gas extraction initiative are situated in areas that are indirectly affected by Russia's aggressive maritime posturing. While the project lies within Romania's EEZ, the proximity of Russian naval activities raises concerns about potential interference, surveillance, or sabotage. The ambiguity surrounding Russia's military exercises, including the declaration of temporary exclusion zones, disrupts commercial operations and creates uncertainty for infrastructure operators in the region.



Hydrocarbons perimeters, Western Black Sea. Source: New Strategy Center

These jurisdictional disputes are further exacerbated by the dual-use nature of maritime infrastructure. Ports, shipping lanes, and offshore platforms often serve both civilian and military purposes, making them attractive targets for hybrid threats. The

[10] EASA Permits Flights on Two Routes Above Black Sea in Simferopol FIR," Center for Transport Strategies, January 25, 2024, https://en.cfts.org.ua/news/easa_permits_flights_on_two_routes_above_black_sea_in_simferopol_fir.

militarization of the Black Sea by Russia, including the deployment of advanced surveillance systems and armed naval forces, has heightened the risk of incidents involving CMI. The legal ambiguities surrounding these activities make it difficult for affected states to respond effectively without escalating tensions further.

In conclusion, hybrid threats are a defining feature of the contemporary security landscape, particularly in the maritime domain. Their ambiguity, adaptability, and multidimensional nature make them a formidable challenge for policymakers and security practitioners. The Black Sea, as a focal point of hybrid operations, offers critical lessons for understanding and addressing these threats. By developing robust and adaptive strategies, states and international organizations can enhance the resilience of critical maritime infrastructure and safeguard global stability.

What is Infrastructure?

Infrastructure is the foundational system that supports societal functions and economic activity, encompassing both physical and organizational structures. In the maritime domain, this includes undersea cables that transmit global internet traffic, offshore platforms extracting oil and gas, wind farms harnessing renewable energy, ports facilitating trade, and shipping lanes connecting global markets. These elements form the backbone of global interconnectivity, ensuring the smooth functioning of economies and societies.

Maritime infrastructure has become increasingly sophisticated, with technological advancements enabling the development of offshore platforms in deeper waters and harsher environments. For instance, undersea data cables, which carry more than 95% of global internet traffic, are vital to communication, finance, and trade. Offshore energy platforms are equally significant, playing a critical role in meeting energy demands and transitioning to renewable energy sources. These infrastructures are not merely passive enablers of global commerce; they are strategic assets that influence geopolitical power dynamics.

Infrastructure is also deeply embedded in legal and normative frameworks, shaping its governance and operation. For example, maritime zones like Exclusive Economic Zones (EEZs) define the rights and responsibilities of states over their adjacent waters. These legal constructs influence how infrastructure is built, maintained, and

protected, while also framing the disputes that arise over contested waters and resources.

Why Is It Important?

Infrastructure's importance lies in its dual role as a driver of economic prosperity and a tool for geopolitical influence. Economically, maritime infrastructure enables global trade, energy production, and communication. Ports serve as critical nodes in supply chains, facilitating the movement of goods and resources. Undersea cables connect continents, enabling real-time financial transactions and communication. Offshore platforms contribute to energy security by reducing dependence on imported energy sources.

Geopolitically, infrastructure serves as a tool for power projection and influence. Nations often use maritime infrastructure to assert control over strategic areas, establish dominance, or foster cooperation. For instance, Romania's Neptune Deep project exemplifies how infrastructure can serve as both an economic asset and a geopolitical tool. The project will become operational in 2027 and will contribute with approximately 8.5 bcm/ year with proven resources of of 160 bcm.This project, situated in the Black Sea, is not only a key component of Romania's energy strategy but also a symbol of its resilience against Russian influence. By providing energy to neighboring countries, Neptune Deep enhances Romania's regional standing and reduces reliance on Russian energy supplies.

Infrastructure also shapes international relations by fostering cooperation or exacerbating tensions. Joint infrastructure projects can strengthen alliances and promote regional stability. Conversely, contested projects, such as the construction of artificial islands in the South China Sea, can heighten geopolitical tensions and lead to conflicts. The dual-use nature of infrastructure, which allows it to serve both civilian and military purposes, further underscores its strategic significance.

Material and Ideational Properties of Infrastructure

Infrastructure possesses both material and ideational properties that influence its role in global politics and security. Materially, infrastructure comprises the physical systems that deliver essential services. For example, undersea cables and offshore platforms are tangible assets that provide communication, energy, and economic

connectivity. The disruption of these systems can have immediate and far-reaching consequences, such as halting financial transactions or disrupting energy supplies.

The material properties of infrastructure are often linked to technological advancements and operational complexities. Offshore platforms, for instance, are highly specialized structures that operate in challenging environments. They require advanced engineering, regular maintenance, and robust security measures. Similarly, undersea cables are vulnerable to physical damage and sabotage, given their placement in remote and unmonitored locations.

Ideationally, infrastructure embodies national aspirations, geopolitical strategies, and societal values. Large-scale projects often serve as symbols of progress, power, and identity. For instance, the Øresund Bridge between Denmark and Sweden represents not only a physical connection but also a symbol of peace and cooperation between two historically adversarial nations. In the Black Sea, the Neptune Deep project represents Romania's ambition to assert its energy independence and regional leadership.

Infrastructure's ideational properties also influence its perception and value. In some cases, infrastructure is seen as a tool for fostering unity and cooperation, as in regional pipeline projects that connect multiple countries. In other cases, it becomes a source of contention, as seen in disputes over resource-rich maritime zones. The symbolic value of infrastructure can amplify its geopolitical significance, making it a target for adversaries seeking to undermine national or regional stability.

The interaction between material and ideational properties is particularly evident in the maritime domain. Offshore platforms and undersea cables, while primarily valued for their functional contributions, also carry significant symbolic weight. They represent technological progress, economic resilience, and geopolitical ambitions. This duality makes them attractive targets for hybrid threats, which aim to exploit both their functional vulnerabilities and their symbolic significance.

Challenges in Protecting Infrastructure

The protection of maritime infrastructure is fraught with challenges. The remote and vast nature of the maritime domain complicates monitoring and enforcement efforts. Legal ambiguities in international frameworks, such as the United Nations

Convention on the Law of the Sea (UNCLOS), further hinder effective governance. Additionally, the dual-use nature of infrastructure increases its susceptibility to exploitation in conflicts.

Hybrid threats exacerbate these challenges by exploiting both material and ideational vulnerabilities. For instance, sabotage of undersea cables not only disrupts communication but also undermines public confidence in the resilience of critical systems. Similarly, attacks on offshore platforms can have cascading effects, disrupting energy supplies and destabilizing economies.

In conclusion, infrastructure is a multifaceted concept that encompasses material assets and ideational dimensions. Its importance lies in its ability to sustain societal functions, drive economic activity, and shape geopolitical dynamics. The protection of maritime infrastructure requires a comprehensive approach that addresses both its physical vulnerabilities and its symbolic significance. As hybrid threats continue to evolve, safeguarding critical infrastructure will remain a central challenge for policymakers and security practitioners.

What Makes an Infrastructure Critical?

Critical infrastructure is defined by its role in sustaining vital societal, economic, and security functions. When the disruption or destruction of a particular system results in widespread consequences, it is deemed critical. This designation applies to systems such as energy grids, transportation networks, communication systems, and, in the maritime domain, undersea cables, offshore platforms, and shipping lanes. These infrastructures underpin not only national economies but also global stability, making them indispensable to modern society.

In the maritime domain, criticality stems from the unique dependence on infrastructures that operate in remote and challenging environments. Offshore platforms provide energy resources that power economies and sustain energy security. Ports and shipping lanes serve as the arteries of global trade, facilitating the movement of goods and resources across continents.

Criticality also arises from the interconnected nature of modern infrastructures. A disruption in one system can cascade into failures across multiple sectors. For example, an attack on undersea cables can halt financial markets, disrupt

communication networks, and compromise national security. Similarly, the sabotage of offshore platforms can destabilize energy supplies, trigger economic shocks, and undermine public confidence in state capabilities. This interconnectedness amplifies the impact of threats to critical infrastructure, making their protection a top priority for policymakers and security practitioners.

Transocean Barents Rig. Source: OMV Petrom

Material and Ideational Dimensions of Criticality

Critical infrastructure is not only defined by its material properties but also by its ideational dimensions. Materially, criticality is determined by the functional importance of infrastructure in maintaining societal and economic stability. For example, the Neptune Deep project in Romania's Exclusive Economic Zone (EEZ) is critical for meeting regional energy demands and reducing dependence on external suppliers. Its material value lies in its capacity to produce energy resources that sustain economic growth and resilience.

However, criticality extends beyond functional utility to encompass the symbolic and strategic value of infrastructure. Ideationally, infrastructure can represent national pride, geopolitical influence, and societal progress. The Neptune Deep project is not only an energy initiative but also a symbol of Romania's regional leadership and resilience against Russian influence in the Black Sea. Its successful implementation would enhance Romania's status as a regional energy hub, while its disruption would undermine public confidence and weaken the country's geopolitical standing.

This duality makes critical infrastructure an attractive target for hybrid threats, which exploit both material vulnerabilities and symbolic significance. Adversaries may target infrastructure to disrupt essential services, but they may also aim to erode public trust, destabilize political systems, or challenge the legitimacy of governing authorities. The ideational value of infrastructure amplifies the impact of such attacks, as they resonate beyond the immediate physical consequences to affect societal perceptions and international relations.

Challenges in Protecting Critical Infrastructure

The protection of critical infrastructure faces numerous challenges. The remote and dispersed nature of maritime infrastructures makes monitoring and defense particularly difficult. Legal ambiguities, such as those surrounding Exclusive Economic Zones (EEZs) under international law, complicate jurisdiction and enforcement. Additionally, the dual-use nature of many infrastructures, such as ports and transport systems, increases their susceptibility to exploitation in conflicts.

Hybrid threats further exacerbate these challenges by targeting both the functional and symbolic dimensions of critical infrastructure. For example, cyberattacks on undersea cables disrupt communication and commerce, while simultaneously signaling vulnerabilities to adversaries. Similarly, sabotage of offshore platforms can destabilize regional energy markets and undermine national resilience.

Criticality is a multifaceted concept that encompasses both the material importance and the symbolic significance of infrastructure. In the maritime domain, critical infrastructure is essential for maintaining economic stability, energy security, and global connectivity. However, its criticality also makes it a target for hybrid threats, which exploit its vulnerabilities to achieve strategic objectives. Addressing these threats requires a comprehensive approach that integrates legal, technological, and strategic measures to protect both the functional and ideational dimensions of critical infrastructure.

Threats to Critical Maritime Infrastructure

The Black Sea offers an important case study for understanding the multifaceted threats to critical maritime infrastructure (CMI) and the lessons that can be applied to protect such infrastructure worldwide. This contested maritime region, with its

complex mix of geopolitical tensions, overlapping territorial claims, and reliance on offshore resources, exemplifies the challenges posed by hybrid threats to energy platforms, undersea cables, and maritime trade routes. By analyzing the threats and key insights drawn from collaborative regional analyses and exercises, stakeholders can identify best practices for enhancing the security and resilience of CMI globally.

Threats to CMI in the Black Sea and other contested regions encompass a spectrum of physical, cyber, and informational challenges. These threats exploit systemic vulnerabilities in infrastructure, creating cascading effects that extend beyond immediate disruptions to economic and societal stability.

Physical Threats

Physical threats involve direct attacks or disruptions targeting maritime infrastructure such as energy platforms, undersea cables, and shipping lanes. These threats can take many forms, from the deployment of drifting mines to covert sabotage operations. For example, drifting mines are a particularly potent threat in contested maritime regions, as they can halt energy production, obstruct maritime navigation, and generate widespread economic disruptions.

The use of Maritime Autonomous Vehicles (MAVs) and Unmanned Aerial Vehicles (UAVs) also presents a significant challenge. These technologies can be employed for covert surveillance, sabotage, or interference with offshore platforms and data cables. The covert nature of MAVs and UAVs complicates detection and attribution, making them ideal tools for hybrid operations in maritime zones. By targeting critical energy infrastructure, these threats not only disrupt production but also create significant risks for regional security.

Cyber Threats

Cyber threats to maritime infrastructure are increasingly prevalent, given the reliance of modern systems on digital technologies and networked controls. Offshore energy platforms, undersea data cables, and shipping operations are highly dependent on Supervisory Control and Data Acquisition (SCADA) systems and other operational technologies (OT) for efficient functioning. These systems, however, are vulnerable to cyber attacks that can disrupt operations and compromise safety.

Examples of cyber vulnerabilities include malware that infiltrates control systems, disrupting energy production or interfering with communication networks. Cyber threats often work in tandem with physical or informational attacks, amplifying their impact. For instance, a coordinated cyber attack on undersea cables could halt financial transactions and disrupt internet connectivity, while disinformation campaigns spread fear and uncertainty among affected populations.

Insights drawn from regional analyses have highlighted the need to integrate robust cybersecurity measures into the protection of maritime infrastructure. This includes the use of advanced monitoring systems, real-time intrusion detection, and rapid response protocols to minimize the impact of cyber incidents.

Informational Threats

Informational threats leverage disinformation, propaganda, and media manipulation to amplify. They can either amplify the effects of physical and cyber attacks or act as standalone tools. By shaping public perceptions and undermining trust in governments or infrastructure operators, informational threats can destabilize societies and exacerbate the consequences of hybrid operations.

For example, disinformation campaigns targeting offshore energy projects may spread exaggerated claims about the vulnerabilities of infrastructure, eroding public confidence and creating political pressure. Such campaigns are often orchestrated through social media platforms and other digital channels, which allow adversaries to reach large audiences quickly.[11] By distorting narratives and exploiting crises, these threats aim to weaken societal resilience and complicate crisis management efforts. Moreover, disinformation campaign can undermine the decision to invest in a project through falsehoods regarding the environmental project or the economic benefits to the local population. In the case of energy projects, prevalent narratives revolve around the selling of the resources to foreign entities to the detriment of national wellbeing and the local population.

Key Lessons for Protecting Critical Maritime Infrastructure

The threats faced by CMI in the Black Sea provide critical lessons for mitigating risks and strengthening the resilience of infrastructure in other regions. These lessons

[11] Daniel Ioniță et al., Norway and Romania: Navigating Information Warfare, ed. Sergiu Mitrescu and George Scutaru (New Strategy Center, 2024).

emphasize the importance of regional cooperation, technological innovation, and comprehensive strategies that integrate physical, cyber, and informational defenses.

Regional Cooperation

Effective protection of CMI requires coordinated action among neighboring states. In contested regions like the Black Sea, where multiple countries share maritime boundaries and resources, regional cooperation is essential for addressing transnational threats. Joint initiatives, such as real-time intelligence sharing and collaborative maritime patrols, can significantly enhance situational awareness and response capabilities.

Lessons from regional analyses underline the importance of establishing frameworks for cross-border cooperation, particularly in the face of hybrid threats that exploit jurisdictional ambiguities. States must develop shared protocols for responding to incidents, conducting joint crisis management exercises, and maintaining open lines of communication to build trust and enhance collective resilience.

MCM Black Sea Task Group
Source: NATO Maritime Command Facebook

Cybersecurity Integration

The integration of cybersecurity into the broader framework of CMI protection is a critical priority. Cyber attacks on maritime infrastructure can disrupt energy systems, paralyze communication networks, and compromise safety. To address these risks,

states and operators must invest in advanced cybersecurity measures, including real-time monitoring, automated intrusion detection systems, and the development of incident response teams.

Additionally, collaborative efforts are needed to strengthen cyber defenses at the regional and international levels. Establishing shared standards and frameworks for cybersecurity, as well as conducting joint cyber defense exercises, can help improve preparedness and ensure a unified response to cross-border cyber threats.

Strategic Communications

The importance of strategic communications cannot be overstated in countering informational threats and maintaining public trust during crises. Hybrid threats often involve the use of disinformation campaigns to exploit vulnerabilities and amplify the effects of physical and cyber attacks. Proactive and transparent communication strategies are essential for dispelling false narratives, addressing public concerns, and demonstrating resilience.

States and infrastructure operators should prioritize the development of strategic communication plans that include partnerships with media outlets, trained spokespersons, and effective use of digital platforms. By ensuring the timely dissemination of accurate information, these plans can help mitigate the impact of disinformation and foster societal confidence in government and private sector responses.

Technological Innovation

Technological advancements offer both challenges and opportunities for protecting CMI. While adversaries may use technologies such as MAVs and UAVs to exploit vulnerabilities, these same tools can be employed for surveillance, early warning, and threat detection. Investment in cutting-edge technologies, including satellite monitoring, autonomous drones, and advanced data analytics, can significantly enhance maritime situational awareness and improve the ability to detect and respond to emerging threats.

For instance, the use of drones for patrolling offshore platforms and monitoring undersea cables provides real-time intelligence on potential threats, enabling rapid

countermeasures. Similarly, satellite systems can track the movement of suspicious vessels and drifting mines, offering critical information for timely intervention.

Legal and Regulatory Reforms

The challenges of hybrid threats are compounded by gaps in legal and regulatory frameworks governing maritime security. Existing international agreements, such as the United Nations Convention on the Law of the Sea (UNCLOS), often fail to address the complexities of modern hybrid operations, leaving states ill-equipped to respond effectively.

Efforts to reform and adapt legal frameworks are essential for addressing these challenges. This includes clarifying jurisdictional ambiguities, enhancing enforcement mechanisms, and developing protocols for responding to cyber attacks, covert operations, and other hybrid tactics. Strengthening legal and regulatory measures provides states with the tools needed to protect their maritime infrastructure and hold perpetrators accountable.

Resilience and Redundancy

Building resilience and redundancy into CMI is a critical strategy for mitigating the impact of hybrid threats. Infrastructure systems should be designed to withstand and recover from attacks, with redundant systems in place to ensure continuity of operations. For example, alternative energy routes, backup communication networks, and diversified energy sources can help reduce the vulnerability of offshore platforms and undersea cables.

Investments in resilience also extend to crisis management capabilities. Conducting regular security assessments, scenario planning, and drills can improve preparedness and ensure that stakeholders are equipped to respond to complex hybrid threats. By fostering a culture of resilience, states and operators can reduce the impact of disruptions and maintain societal confidence in the face of adversity.

Conclusion

The Black Sea region highlights the evolving threats to critical maritime infrastructure and the need for comprehensive strategies to address them. Hybrid threats that combine physical, cyber, and informational dimensions pose complex challenges that require integrated responses. Lessons drawn from regional experiences emphasize the importance of cooperation, technological innovation, strategic communication, and legal reform in mitigating these risks.

However, beyond the security dimension, critical maritime infrastructure in the Black Sea is deeply intertwined with the geopolitical and economic transformations taking place in the region. One of the most significant shifts is the diversification of energy sources and the reduced dependence on Russian energy. Historically, Russia has used energy as a tool for political leverage, exerting pressure on dependent nations through supply cuts, price manipulation, and politically motivated infrastructure disruptions. The emergence of alternative energy sources in the Black Sea, particularly offshore gas projects like Neptune Deep in Romania and the expansion of Bulgaria's gas production capabilities, marks a strategic turning point.

For Romania, increasing domestic gas production not only strengthens its energy security but also elevates its regional strategic relevance. Over the next decade, Romania is poised to become a key energy player in Southeast Europe, capable of supplying gas to neighboring countries and reducing their vulnerability to Russian coercion. Similarly, Bulgaria's transition from an energy importer to an exporter could reshape its geopolitical posture, allowing it to play a more autonomous role in regional energy dynamics.

Beyond the direct energy-producing nations, the ripple effects of these changes will extend to other European states, particularly those seeking to diversify their energy imports. Germany, for example, has already signed an agreement with OMV Petrom to receive gas from the Black Sea after 2027. This reflects the broader European effort to reduce reliance on Russian hydrocarbons and secure stable energy supplies from alternative sources. As new energy corridors emerge, regional cooperation will deepen, with countries such as Bulgaria, Turkey, and Romania strengthening their collaboration, with the mine countermeasure MoU expected to be expanded to cover offshore critical infrastructure.

The protection of critical maritime infrastructure will play a crucial role in facilitating this transition. Ensuring the security of offshore platforms, undersea pipelines, and gas transit corridors will be essential for maintaining the stability of emerging energy networks. This imperative is already driving enhanced regional cooperation, with countries such as Bulgaria, Turkey, and Romania intensifying joint security initiatives in the Black Sea. Moreover, the geopolitical stakes of Black Sea energy resources are likely to attract greater involvement from external actors, including the European Union and NATO, which have a vested interest in securing alternative energy supplies.

In conclusion, the protection of critical maritime infrastructure in the Black Sea is not just a matter of security but a pivotal factor in reshaping regional energy politics. As countries transition away from Russian energy dependence, new economic and strategic opportunities will emerge, reinforcing regional alliances and strengthening Europe's resilience against external pressures. By safeguarding these infrastructures, Black Sea states can accelerate their energy independence, enhance their geopolitical influence, and contribute to a more stable and diversified European energy landscape.

Bibliography

- Bertrand, Natasha, Oren Liebermann, and Haley Britzky. “Russian Fighter Jet Forces Down US Drone Over Black Sea After Intercept.” *CNN*, March 14, 2023.

- Eurocontrol. *Flight Information Region (FIR/UIR) Charts 2024.* Eurocontrol, 2024. https://www.eurocontrol.int/publication/flight-information-region-firuir-charts-2024.

- Hoffman, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars.* Arlington, VA: Potomac Institute for Policy Studies, 2007.

- Ioniță, Daniel, Ion Cristea, Cristina Melnic, Remus Ștefureac, Jakub M. Godzimirski, and Matthew Blackburn. *Norway and Romania: Navigating Information Warfare.* Edited by Sergiu Mitrescu and George Scutaru. New Strategy Center, 2024. https://newstrategycenter.ro/project/norway-and-romania-navigating-information-warfare-2/.

- Pickrell, Ryan. “17 Russian Jets Buzzed a British Destroyer in the Black Sea.” *Business Insider*, November 2, 2018.

- “Razboiul Rusiei împotriva Ucrainei: Nave rusești, dar și o mină, s-au apropiat periculos de cea mai nouă platformă petrolieră românească din Marea Neagră.” *Profit.ro*, January 23, 2024.

- “Russia Intercepts Polish Jet Over Black Sea in ‘Aggressive and Dangerous’ Maneuver, Warsaw Says.” *Radio Free Europe/Radio Liberty (RFE/RL)*, May 7, 2023.

- Scutaru, George, and Peter Watkins**.** *Security Challenges in the Black Sea: NATO, the Wider Region, and the Global Order – Pledging for a Free and Open Black Sea.* New Strategy Center, 2023. https://newstrategycenter.ro/project/security-challenges-in-the-black-sea-nato-the-wider-region-and-the-global-order-pledging-for-a-free-and-open-black-sea/.

- Scutaru, George, Antonia Colibasanu, Matthew Boyse, and Mykhailo Samus. *The Battle for the Black Sea Is Not Over.* New Strategy Center, 2024. https://newstrategycenter.ro/project/the-battle-for-the-black-sea-is-not-over/.

- Temnycky, Mark. “British Warship Challenges Russian Claims to Crimea.” *Atlantic Council*, June 25, 2021.

- “EASA Permits Flights on Two Routes Above Black Sea in Simferopol FIR.” *Center for Transport Strategies*, January 25, 2024.

ISBN: 978-606-95860-2-0

Follow us on social media:

NSC_Romania
New Strategy Center - NSC
office@newstrategycenter.ro
https://newstrategycenter.ro/en/home/
New Strategy Center

NEW
STRATEGY
CENTER