

RISK MANAGEMENT IN NAVAL COMBAT OPERATIONS UNDER ASYMMETRIC THREATS: IMPLICATIONS FOR BLACK SEA SECURITY

Pavlo Rud
*Institute of Naval Forces
National University "Odesa Maritime
Academy"
Odesa, Ukraine*

Abstract. The security architecture of the Black Sea region is increasingly shaped by asymmetric threats that challenge conventional naval superiority and alter the logic of maritime risk management. The proliferation of unmanned systems, cyber operations, hybrid tactics, anti-access/area denial (A2/AD) strategies, and irregular maritime actors has transformed the operational environment into a multidomain risk space. This paper examines the theoretical foundations and practical application of risk management in naval combat operations under asymmetric conditions, with particular reference to the Black Sea theater. It analyzes the evolving character of asymmetric maritime threats, evaluates existing risk management frameworks, and identifies tactical, operational, and strategic mitigation mechanisms. Special attention is given to cyber resilience, distributed command-and-control systems, predictive analytics, and multinational maritime cooperation. The study argues that effective naval risk management in the Black Sea requires adaptive, technology-enabled, and alliance-integrated approaches capable of transforming asymmetric vulnerabilities into controlled operational risks. The findings highlight the necessity of doctrinal innovation, multidomain integration, and strategic coordination among regional maritime stakeholders.

Keywords: *asymmetric threats; Black Sea security; naval warfare; risk management; A2/AD; cyber resilience; maritime strategy.*

Background

The contemporary maritime security environment in the Black Sea region has entered a phase of structural transformation. Unlike traditional symmetrical naval competition, current dynamics are characterized by asymmetric confrontation, where technologically inferior or numerically weaker actors employ unconventional methods to offset conventional disadvantages.

Asymmetric threats in the maritime domain include unmanned aerial and maritime systems, precision-guided munitions, cyberattacks, electronic warfare, hybrid maritime tactics, mine warfare, and information operations conducted below the threshold of declared hostilities (Kumar 2010). These instruments create a multidimensional battlespace that challenges traditional naval risk assessment models.

The Black Sea has emerged as a laboratory of modern asymmetric naval warfare. The integration of unmanned systems, coastal missile complexes, maritime drones, cyber disruption, and distributed intelligence has redefined operational risk parameters. Consequently, risk management in naval combat operations is no longer confined to kinetic engagements but extends to digital, informational, and strategic domains.

This paper aims to analyze how risk management frameworks must adapt to asymmetric threats and to identify implications for naval operations and regional security in the Black Sea.

1. The Nature of Asymmetric Maritime Threats

Asymmetric threats are defined by the exploitation of vulnerabilities in superior conventional forces through non-traditional methods. In maritime environments, such tactics include swarming fast attack craft, unmanned surface and aerial systems, covert mine deployment, electronic disruption, and cyber interference (Kimpel 2006).

In strategic chokepoints such as the Strait of Hormuz, integrated A2/AD architectures demonstrate how layered missile systems, drone operations, and maritime denial tactics create

complex operational risk environments (Shapira 2025). Similar patterns are observable in the Black Sea, where coastal missile systems and maritime drones significantly influence naval maneuverability.

The A2/AD paradigm limits operational freedom and imposes strategic constraints on maritime actors. These mechanisms shift the risk calculus from fleet confrontation to distributed, network-centric engagements.

2. Risk Management Frameworks in Naval Operations

Classical military risk management involves identification, assessment, mitigation, and monitoring. However, asymmetric maritime threats require multidomain integration.

Cybersecurity has emerged as a critical dimension of naval risk management. Research on shipboard operational technology systems highlights the vulnerability of navigation, propulsion, and communication systems to cyber intrusion (Rajaram, Goh, Zhou 2022). Comparative cyber risk analyses confirm that maritime platforms require layered digital defense architectures.

Maritime cybersecurity scholarship emphasizes that cyber threats directly affect operational safety and navigational integrity (Zayats 2019). In the Black Sea context, where electronic warfare and digital interference are prevalent, cyber resilience is inseparable from combat readiness.

Integrated adaptive safety management models further demonstrate the value of simulation-based forecasting and predictive modeling for assessing dynamic risk scenarios (Nikitiuk, Melnyk 2025). Such tools enhance commanders' ability to anticipate adversarial adaptation.

3. Tactical and Operational Adaptation

3.1 Tactical Level

At the tactical level, asymmetric risk mitigation requires rapid detection, distributed decision-making, and integration of unmanned systems. Swarm tactics and maritime drones aim to overwhelm defensive systems and saturate sensors (Kimpel 2006).

Countermeasures include layered air and missile defense, electronic countermeasures, decentralized C2 nodes, and flexible maneuver doctrines. Reducing reaction time and increasing system redundancy are critical for maintaining survivability.

3.2 Operational Level

Operational risk management depends on real-time intelligence fusion. Multisource ISR integration enhances situational awareness and supports predictive risk modeling (Nikitiuk, Melnyk 2025). Scenario-based operational planning allows commanders to evaluate courses of action under uncertainty. Data-driven risk matrices improve resource allocation and enhance resilience in contested maritime environments.

4. Strategic Implications for Black Sea Security

Strategic risk management transcends immediate battlefield concerns. It encompasses alliance interoperability, legal norms, deterrence posture, and regional coordination mechanisms.

Multinational maritime cooperation enhances collective resilience. Strategic doctrine emphasizes forward presence, partnership-based security, and cooperative maritime governance (Conway, Roughead, Allen 2015). In the Black Sea region, coordinated maritime surveillance, intelligence sharing, and joint exercises contribute to risk mitigation.

The proliferation of A2/AD capabilities in the region necessitates integrated responses combining naval maneuver, air defense, cyber protection, and diplomatic coordination. Effective strategic risk management requires balance between deterrence and escalation control.

5. Lessons for Future Naval Risk Management

Recent maritime conflicts demonstrate that asymmetric tools can effectively challenge conventionally superior fleets. Maritime drones, precision strikes, distributed sensor networks, and cyber operations have redefined operational vulnerabilities.

Three key lessons emerge:

1. Technological Adaptability – rapid integration of unmanned and digital systems is essential.

2. Organizational Flexibility – decentralized command enhances resilience.
3. Alliance Integration – regional security frameworks reduce systemic risk.

In the Black Sea context, sustained maritime security depends on the institutionalization of adaptive risk management mechanisms across tactical, operational, and strategic levels.

Conclusion

Risk management in naval combat operations under asymmetric threats requires a multidomain and adaptive framework. The Black Sea region exemplifies how unmanned systems, cyber operations, A2/AD architectures, and hybrid tactics reshape maritime security dynamics.

Traditional naval superiority alone no longer guarantees operational freedom. Instead, strategic advantage derives from the ability to anticipate, quantify, and mitigate complex risks through technological innovation, predictive analytics, cyber resilience, and multinational cooperation.

The transformation of asymmetric threats into manageable operational variables is the defining challenge for contemporary naval strategy in the Black Sea security architecture.

References

Black Sea Harmony., (n.d.). Naval operation for asymmetric threat deterrence. Available from: Operation Black Sea Harmony — Wikipedia Republished // WIKI 2 . [Viewed 2022-5-10].

KIMPEL, J., 2006. *Countering asymmetric threats in the littoral maritime environment*. Available from: https://www.researchgate.net/publication/235096318_Countering_Asymmetric_Threats_in_the_Littoral_Maritime_Environment.

SHAPIRA, B., 2025. *The Iranian Threat to the Strait of Hormuz*. Available from: <https://israel-alma.org/the-iranian-threat-to-the-strait-of-hormuz/>. [Viewed 2025-9-3].

KUMAR, K., 2010. *Asymmetric threats and their challenges to freedom of navigation*. WMU Dissertation. Available from: https://commons.wmu.se/all_dissertations/421/.

NIKITIUK, P.; MELNYK, O., 2025. *Integrated model of assessment and adaptive management of operational safety of a sea vessel in a dynamic environment*. Available from: <https://www.semanticscholar.org/paper/Integrated-model-of-assessment-and-adaptive-of-a-Nykytyuk-Melnyk/ab74ddd39d2152c384b9dc4149b91ed31d505412>. [Viewed 2025-6-30].

RAJARAM, P.; GOH, M.; ZHOU, J., 2022. *Guidelines for cyber risk management in shipboard OT systems*. Available from: https://www.researchgate.net/publication/362483966_Guidelines_for_cyber_risk_management_in_shipboard_operational_technology_systems.

CONWAY, J.; ROUGHEAD, G.; ALLEN, T., 2015. Naval War College Review, Vol. 61, No. 1 , pp. 7-19 . *A cooperative strategy for 21st century seapower*. Available from: <https://www.jstor.org/stable/26396894>.

ZAYATS, S., 2019. *Ensuring maritime security and measures against cyber threats and cyber piracy at sea*. Available from: https://www.researchgate.net/publication/369727546_zabezpecenna_morskoi_bezpeki_ta_zahodi_protidii_kiberzagrozam_ta_kiberpiratstvu_na_mori.