Policy Research Journal
ISSN (E): 3006-7030 ISSN (P) : 3006-7022 Volume 3, Issue 7, 2025

SEA AS A SYSTEM: A MOSAIC-BASED ANALYSIS OF HYBRID MARITIME THREATS

Syeda Fizzah Shuja

Research Associate, Maritime Centre of Excellence (MCE), Pakistan Navy War College (PNWC), Lahore

fizzasyed2k@gmail.com

DOI: https://doi.org/10.5281/zenodo.15788496

Keywords
Hybrid Warfare, Maritime Hybrid Threats, MOSAIC Model, Lawfare, Maritime Domain Awareness, Asymmetric Naval Threats, Strategic Disruptions

Article History
Received on 26 May 2025
Accepted on 26 June 2025
Published on 02 July 2025

Corresponding Author: * **Syeda Fizzah Shuja**

Abstract

As the concept of hybrid warfare introduces a next-generation variant of maritime security, the maritime domain operations are becoming increasingly entangled in complex security dynamics. Hybrid warfare in the maritime domain encompasses a blend of traditional naval operations and unconventional tools such as maritime terrorism, cyber-attack, disinformation, and economic coercion targeting vital sea-based settings, including shipping lanes, undersea critical infrastructure, and deep-sea installations. Moreover, the hybrid threat spectrum covers a subtle yet potent tool for leveraging ambiguous legal maritime regimes, especially in the case of interpreting an Exclusive Economic Zone (EEZ). Reconceptualizing the blue sphere as an interconnected system vulnerable to evolving hybrid tactics, this research draws upon the MOSAIC model, which offers a systematic study of such threats to examine how states preempt, dislocate, or disrupt their adversaries. Using qualitative methods along with region-based case study analysis, this research paper explores the existing gaps in legal maritime infrastructure and regional maritime security framework and highlights strategic gaps in deterrence and attribution. As the existing threat environment of the world is rapidly transforming, this study argues that current traditional and monolithic platform-centric models of maritime defense are insufficient in addressing such issues. In this regard, this paper calls for a multi-domain-based response emphasizing interoperability, distributed deterrence, and network-centric capabilities. Finally, this study concludes by proposing strategies emphasizing multi-domain awareness and interstate coordination to build a resilient response mechanism to the next-generation maritime hybrid threats.

INTRODUCTION

"The supreme art of war is to subdue your enemy without fighting the war." (TZU, 500 BC) The changing character of warfare has evolved beyond the conventional front lines and now manifests through ambiguous, often non-attributable tactics in the contemporary security environment. The transformation is more evident within the maritime domain. Hybrid threats, ranging from disrupting undersea critical infrastructure in the South China Sea (SCS) to cyber intrusions on the targeted Southeast Asian ports, demonstrate the propagation of conflict into the gray zones. These emerging trends attest to the characteristics of hybrid warfare, which include the manipulation and exploitation of structural or strategic deficiencies of adversarial states without crossing the traditional thresholds of war (Bilal, 2021).

The circumvention of the direct conflict enables the actors to conserve their resources while maintaining a

strategic pressure on their adversaries and putting them on guard. This tactic of indirect conflict forces the other state into a state of constant vigilance, where legal, diplomatic, and informational domains are tactically exploited (Wither, 2020). Moreover, such tactics give states and non-state actors a way to project power by disrupting economic stability and eroding maritime domain awareness without actually utilizing the tools of direct kinetic warfare. In addition to the tangible operational advantage, this kind of warfare offers political utility, particularly in the geopolitical climate where overt aggression may provoke international condemnation or trigger rapid escalation beyond control.

Unlike conventional military threats, these hybrid warfare tactics exploit the vulnerabilities of modern maritime systems, which are technologically complex and legally contested these days. Such non-kinetic measures revolve around deniability with increased psychological impact and the ability to create strategic pressure, making the sea a congested system. Additionally, in today's complex security environment, state and non-state actors have made hybrid threats a pertinent component of their broader warfare strategy to achieve their interests (Bargués & Bourekba, 2022).

In this regard, this research addresses how hybrid threats materialize within the maritime domain and, further, how the MOSAIC (military, operations, strategy, asymmetrical, information and cyber) model better explains the emerging strategic pattern all over the world. It critically analyzes the existing maritime security models built around monolithic, platform-centric doctrines, which are insufficient to deter the multidimensional and adaptive nature of maritime hybrid warfare (Jensen & Peschkwitz, 2019). The application of the MOSAIC model frames the maritime domain as a multi-layered field in which increased interconnectedness leads to more instability.

The significance of this study lies in its interdisciplinary approach that bridges strategic studies and regional security, which offers a novel approach in understanding such an evolving character of warfare. Given the increasing importance of maritime chokepoints, critical infrastructure, and sea-based communication systems as national assets, the inability to detect and deter the gray zone tactics poses a serious threat to peace and security in the region. This study intends to contribute to expanding the discourse of hybrid warfare and its maritime manifestation, since this area has been overlooked despite its growing strategic salience. Employing qualitative methodology while examining selected case studies across the Indo-Pacific region, this research aims to highlight the legal, structural, and operational gaps that hybrid actors exploit. Furthermore, this study proposes strategic responses built upon maritime domain awareness and interstate coordination backed by a resilient legal framework.

Maritime Hybrid Warfare

The dynamic reconfiguration of modern warfare has increasingly blurred the traditional boundaries between peace and conflict, combatants and civilians, and simultaneously, between state and non-state actors. The growing ambiguous nature of the maritime battlespace has become a pertinent theater for hybrid operations (Korybokyo, 2015). Hybrid operations may include conflicts engineered to disrupt the adversarial state internally to achieve strategic objectives through asymmetric, ambiguous, and multi-domain tactics without crossing the threshold of conventional warfare.

The term “hybrid warfare” was introduced into academic as well as military discourse by Frank Hoffman, the American strategist. While earlier concepts like “unrestricted warfare,” “compound warfare,” and “fourth-generation warfare” laid the groundwork for similar dynamics, nevertheless, Hoffman framed the whole concept by systematically merging the conventional military force with irregular tactics, cyber operations, and psychological manipulation. Intrinsically, hybrid warfare is defined by its multidimensional nature and layered application (Fridmen, 2018).

Concurrently, the experiential model explains the hybrid influence in two primary phases: the primary phase and the operational phase. The primary phase involves continuous surveillance and observation layered with subtle influence campaigns and the covert development of operational assets. During this period, the actor often deliberately withholds direct aggression while continuously shaping the information environment, testing the legal boundaries, and creating a foundation for escalation.

Once the strategic environment has been prepared, the hybrid actor progresses towards the operational phase, which is characterized by more assertive actions that formulate strategic effects while maintaining plausible deniability. This two-staged channel enables the actors to destabilize adversaries incrementally, without getting into full-scale war (The European Hybrid Centre Of Excellence for Countering Hybrid Threats, 2019).

Drawing its strength from factors like strategic ambiguity, a hybrid actor adapts swiftly between different modes of conflict, including conventional military force, insurgency tactics, criminal activity, terrorism, and even economic subversion. Further to producing cumulative effects across physical, informational, and psychological dimensions of warfare, these modes are operationally synchronized. Simultaneously, a single hybrid unit may launch small-scale kinetic raids in tandem with disseminating disinformation to malign trust in state institutions. Here, the objective is defined merely by the erosion of resilience, cohesion, and response capacity of the target state or institution to degrade the target's internal stability (Ball, 2023).

When such tactics are applied in the maritime domain, the dynamics become significantly more complex due to its vastness, legal ambiguity, and strategic centrality. Maritime spaces, unlike land-based theaters, are governed by overlapping regimes of international law, which are subject to divergent interpretation and contested enforcement (Hybrid Warfare on the High Seas - ICWA, 2025). Ambiguities embedded in the United Nations Convention on the Law of the Sea (UNCLOS), particularly concerning the delineation of Exclusive Economic Zones (EEZs) and territorial waters, have given rise to operational grey zones. The legal uncertainties constrain the enforcement mechanisms and undermine the credibility of a deterrent posture, allowing the hybrid actors to operate covertly and strategically exploit legal loopholes (The European Hybrid Centre Of Excellence for Countering Hybrid Threats, 2019).

In this context, it is observed that the typical hybrid maritime operations occur in the littoral zones where law enforcement capabilities are often overstretched or where the state jurisdiction is more contested. Here comes the utilization of civilian assets in place of any identifiable naval vessels as dual-use platforms: tramp steamers, fishing fleets, light tankers, and even small skiffs become instruments of strategic coercion (Cullen, 2017). Such vessels are difficult to monitor in the congested sea lanes as they seamlessly blend into the commercial traffic. This operational blending creates space for states to exert influence through pressure tactics such as ramming, shadowing, jamming, or blocking movement, without the political consequences of deploying conventional naval assets.

For instance, the proficient deployment of "white hull" coast guard vessels by China and Iran, nominally civilian maritime law enforcement bodies, undertakes strategic actions, yielding operational military impact (White, Black or Red, Coast Guard Needs New Hulls – Professional Mariner, 2021). These operations are often manned by non-uniformed personnel, also known as "little blue sailors," who mirror the role of Russia's "little green men" in Crimea. Such staff carry no insignia or clear identification and may disclaim formal affiliation, strategically positioned in the grey area between civilian and military status, enabling their sponsoring states to deny responsibility and delay international reaction (Orbaiceta, 2023).

In the present era, unmarked vessels are rapidly transforming into modular combat systems that may carry a diverse configuration of concealed weaponry, including light arms, heavy-caliber mounted machine guns, shoulder-fired missiles, acoustic weapons, laser dazzlers, and other non-lethal devices suited for escalation control. These vessels carry out operations relying on decentralized and off-the-shelf command and control architectures, impairing the ability to intercept or disrupt such operations (STAVRIDIS, 2016). Not only that, these vessels possess the ability to deploy unmanned aerial and underwater sensors, lay down sonobuoys, or place seabed sensor nodes, cultivating a quiet surveillance system beneath the surface of the sea.

At a more advanced level, the deployment of commercial-looking vessels modified for combat (Q-ships) demonstrates the next phase of evolution of maritime hybrid platforms. Operating under the guise of merchant vessels, these ships can clandestinely carry missile launchers or lay maritime improvised explosive devices (MIEDs) such as untraceable sea mines (Hawkin, 2017). Such capabilities equip the hybrid actors to initiate escalation under the radar,

induce strategic surprise, and incapacitate adversaries' decision-making processes, often with minimal cost and limited direct engagements.

The potential targets of such an operation may focus on critical maritime infrastructure, including offshore oil and gas platforms, underwater hydrocarbon pipelines, subsea data cables, shipping terminals, and, increasingly, deep-seabed mining installations. While indispensable to economic continuity, these assets remain elusive to comprehensive protection efforts in the contested waters.

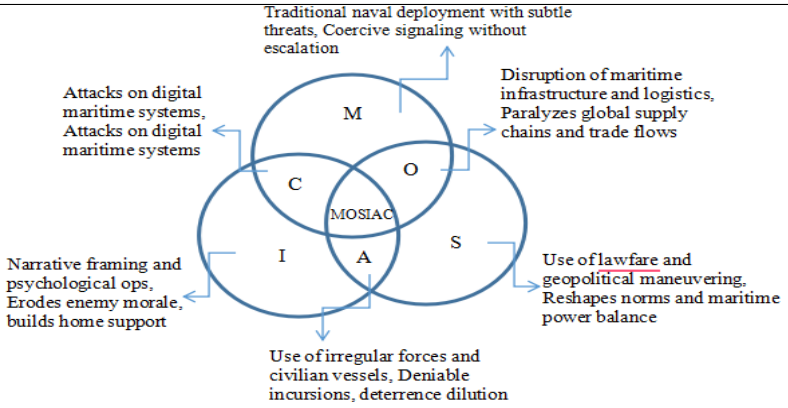
In essence, maritime hybrid warfare follows the approach to strategically weaponize the existing ambiguity in the sea. It is to channelize the tactics to subvert the maritime order, triggering conventional responses, and its success lies in the intrinsic interplay of operational flexibility, plausible deniability, and the exploitation of legal grey zones. In reality, hybrid threats treat the sea not as a void lacking strategic agency but as an active system. Therefore, to comprehensively assess the scope and impact of hybrid threats, it is pertinent to approach the sea as a system where vulnerabilities are not isolated but systemic.

Theoretical Integration of MOSAIC in Maritime Hybrid Warfare Analysis

The shift from rigid, monolithic maritime defense models toward adaptive, networked force architectures marks a pivotal transformation in the way hybrid warfare at sea is conceptualized and conducted. In contrast to conventional doctrines centered around large, centralized naval platforms, the MOSAIC warfare model, introduced by the Defense Advanced Research Projects Agency (DARPA), proposes a framework that offers strategic superiority by design. Rather than relying on singular high-value targets, the model advocates for the use of modular, disaggregated "tiles," including manned and unmanned systems, autonomous platforms, cyber tools, and electronic warfare capabilities. Collectively, these tools can be orchestrated in response to the specific demands of multi-domain engagements (DARPA Tiles Together a Vision of Mosaic Warfare, 2019).

Within the maritime context, this approach addresses a critical limitation of traditional naval security paradigms: their inability to respond to simultaneous, low-signature, and non-attributable threats that often fall below the threshold of open conflict. The MOSAIC model's emphasis on heterogeneity and composability means that hybrid actors can structure their actions across various domains (military, legal, informational, and cyber) while remaining agile and difficult to deter (Jensen, 2019). This mirrors operational realities in the maritime domain, where hybrid maritime warfare increasingly consists of asymmetric tactics such as cyber-enabled sabotage, strategic lawfare, and gray-zone maneuvers within contested Exclusive Economic Zones (EEZs).

Crucially, the MOSAIC model does not treat these hybrid tactics as isolated phenomena. Instead, it understands them as part of an orchestrated effects web, where interdependencies between modular units (unmanned vehicles, satellite-linked drones, legal tools, or data manipulation) allow for the rapid creation of tailored pressure points. The six interlocking domains of MOSAIC (Military, Operational, Strategic, Asymmetric, Information, and Cyber) collectively map the architectural logic of this model. Each domain contributes to a larger operational tapestry that challenges adversaries not through brute force, but through operational complexity- what DARPA terms "complexity as asymmetric advantage." (O'Donoughue et al., 2021)



In the military and operational domains, for example, traditional deterrence postures are diluted by the deployment of low-cost, low-visibility assets such as Q-ships, fishing militias, and dual-use coast guard vessels. These units operate in congested maritime corridors, exploiting attribution gaps while masking intent—hallmarks of a disaggregated force structure. Strategically, these actions are often legitimized through reinterpretations of international law (notably UNCLOS), illustrating how lawfare becomes a modular component of hybrid engagement. In parallel, the informational domain compounds the challenge by shaping public perception and delegitimizing adversarial responses (Jensen, 2019).

The cyber domain, likewise, plays a critical role in hybrid maritime conflict. Threats to undersea cables, port logistics systems, and naval communication networks can yield disproportionate strategic outcomes (Missiroli, 2022). Such cyber incursions are rarely isolated; they are often synchronized with kinetic, legal, or informational operations, validating the MOSAIC model's assertion that modular units must be interoperable and dynamically reconfigurable to achieve strategic depth.

Moreover, the AI-enabled integration principle central to MOSAIC allows for accelerated decision-making cycles (OODA loop dominance) and multi-domain coordination. In environments where maritime awareness is challenged by high traffic density, spoofed identities, and deceptive signaling, AI-supported sensing and rapid decision architectures become vital to detecting, interpreting, and responding to hybrid activities in real time. This technological scaffolding enables decentralized command structures to operate with flexibility while retaining strategic coherence (Deptula & Penny, 2019).

Experimental findings from DARPA's strategic wargaming further reinforce this logic. In simulated Anti-Access/Area Denial (A2/AD) and littoral environments, conditions that closely resemble contemporary Indo-Pacific scenarios, forces structured along MOSAIC principles demonstrated superior resilience, responsiveness, and survivability. The use of autonomous maritime swarms, integrated cyber-electromagnetic attack modules, and AI-driven targeting systems allowed these units to generate parallel effects across physical and digital seaspace, overwhelming adversarial systems not through volume, but through complexity and adaptability. (Clark et al., 2020)

In essence, the MOSAIC model offers both a theoretical and operational bridge between the fragmented realities of hybrid maritime conflict and the strategic imperative for agile defense structures. By adopting MOSAIC as the conceptual framework for this research, the study reframes maritime security as a layered, system-of-systems challenge, requiring modular responses that are fast, dynamic, and legally cognizant.

Multi-Layered Dimensions of the Sea as a System

Framing the "sea as a system" indicates a mosaic of interdependent layers, including geophysical, informational, economic, and social, all of which hybrid actors or aggressors seek to infiltrate or weaponize. This statement acts as a diagnostic of how a maritime domain must be understood in the face of complex and multidimensional challenges. The long-held view of the sea as a neutral expanse regulated by

maritime laws and contested by naval power no longer prevails. In an era where maritime threats mutate faster than our response, and to comprehend the shifting dynamics of global maritime security, redefinition of the seas as a system is necessary as a layered construct driven by multiple actors, intersecting jurisdictions, and systematic vulnerabilities.

For much of modern history, maritime strategic thinking had been grounded in territorial and naval-centric paradigms. From Mahan's emphasis on control of strategic choke points and attaining sea power (Milestones in the History of U.S. Foreign Relations, n.d.) to the Cold War strategists' reliance on naval deterrence doctrines, the prevailing focus remained mainly state-centric and kinetic. However, such thinking falls short in accounting for the systematic complexity of today's maritime security realities. Today, the sea is not just a physical domain of naval maneuvering but constitutes a multidimensional space where aspects like energy flows, legal norms, digital data, migration, and information converge and intersect. In this way, treating maritime issues as discrete domains (e.g., piracy, smuggling, naval escalation) brushes past the interconnected nature of newly emerging threats. On this point, the systems approach deals with the events in layers, like an attack on infrastructure that can cascade through legal, economic, and informational domains.

The foundational layer of the system is the geophysical and infrastructural layer, which includes its geography, seabed topology, and infrastructure. Yet, this first layer has hidden political and technological fault lines. Consider the Nord Stream sabotage (2022). This deliberate disruption of the Baltic undersea pipeline extended far beyond the environmental and energy issues, as this event simultaneously triggered regional insecurity and jolted NATO to reconsider subsea domain awareness (Tebel, 2023). Along the same lines, there lies an intricate web of global undersea cable networks that transmits nearly 95% of the world's data. Whether caused by natural disasters or deliberate sabotage, any damage to such can cripple critical digital and financial systems, causing the loss of trillions of dollars annually. The Svalbard Cable incident (2022) was a wake-up call, exposing the fragility of secure connectivity beneath the waves (Shuja, 2024).

The legal layer, centered around the United Nations Convention on the Law of the Sea (UNCLOS 1982), further reinforces the legal-systematic character of the sea. However, the convention's inherent ambiguities are rapidly weaponized by hybrid actors. The 2016 arbitrary ruling of the South China Sea (SCS) legally invalidated China's "nine-dash line" claims, which remain unenforced. Despite the verdict, China continues to assert control and register its presence through coast guards, artificial islands, and fishing militias (Soares, 2025). This highlights how legal gray zones morph into operational enablers for strategic leverage in the name of protection of sovereignty, blurring the lines between legal posturing and tactical coercion. In a system-based view, such practices are not confined to a single legal breach but can have certain ripple effects across resource control and naval diplomatic posture.

Likewise, the maritime domain acts as a backbone to the global economy as it facilitates carrying out over 90% of world trade via maritime routes and also holds huge reserves of untapped critical energy resources (Shipping and World Trade: World Seaborne Trade, 2024). Adding another layer to the system, maritime economic stability is becoming more susceptible to manipulation and coercion. Just recently, Houthi strikes in the Red Sea compelled major shipping companies to abandon the Suez Shortcut for the longer route around the Cape of Good Hope. This trade route transition caused a tremendous increase in freight charges and contributed to jammed or delayed supply chains (Raydan, 2023). Same, just like that, port projects such as Sri Lanka's Hambantota reveal how debt-trap diplomacy can transform maritime infrastructure into the convergence of economic dependency, transferring not just fiscal control but also extending geopolitical influence (Debunking the Myth of 'Debt-Trap Diplomacy' | 4. Sri Lanka and the BRI, 2020). Consequently, such disruptions are not merely economic anomalies; in fact, they are manifestations of strategic leverage to exert political pressure by the instrumentalization of the maritime economic layer.

Equally important is the cognitive layer of the maritime system, i.e., informational ambiguity under the scope of hybrid maritime threats. In current

circumstances, firm control over information, giving birth to divergent perceptions and narratives, is as important as control over territory. Therefore, tactics like AIS (Automatic Identification System) spoofing, information campaigns, deep-sea jamming, and false flag operations in maritime zones have become progressively common as tools of strategic influence (Mehmood & Malik, 2021). Against this setting, Russian vessels allegedly suspected of GPS jamming in the closer proximity of the NATO coastline (Russia Accused of Jamming GPS Navigation, 2024), alongside China's carefully carved strategic messaging surrounding US naval exercises FONOPS as provocations, exemplify how states pursue perception management and control the narratives shaping both domestic and international responses (Panda, 2018). In such cases, the deliberate denial of attribution, the invocation of alternative legal frameworks, and the orchestration of ambiguity function as instruments of soft coercion.

Perhaps most often neglected in traditional maritime analysis is the socio-political layer. Maritime space is inhabited and politicized by civilian actors such as coastal communities, fishermen, port workers, and even migrants. This human dimension is the most volatile one that can either be leveraged or severely disrupted. The 2014-2016 Mediterranean migrant crisis serves as a striking example of how the sea became a political battleground where rescue met resistance in the name of prioritizing national security. Not only that, even maritime mobility was weaponized by both the state and smugglers to put pressure on the government (McGowan, 2023). Likewise, China's attempt to deliberately obscure the boundary between civil and military domains by deploying a civilian fishing fleet to reinforce its maritime claim challenges the established rules of engagement (Davidson, 2024). When this layer disrupts, consequences get systemic, i.e., human security, disrupt coastal communities, and domestic political backlash.

Understanding the sea as a system is an operational necessity for anticipating, mitigating, and responding to the evolving hybrid challenges that threaten maritime security on a global scale.

Emerging Strategic Pattern at Sea

Having framed maritime hybrid warfare through the MOSAIC model, recent shifts in the maritime threat environment reveal patterned behaviors that exploit the interconnectedness of sea-based infrastructure, legal ambiguity, and digital networks.Understanding these trends is essential for mapping how hybrid strategies are calibrated to exploit the very structure of the maritime system.

1. Ambiguity and Deniability

At the heart of maritime hybrid warfare lies strategic ambiguity, a deliberate erosion of clarity in intent and identity. Unlike conventional naval encounters governed by flags, uniforms, and open declarations, hybrid actors thrive in legal and political grey zones. By deploying vessels without state insignia, operating through opaque networks, and utilizing legally ambiguous claims, states can project power while maintaining plausible deniability (Mumford & Carlucci, 2022, #192).

The Scarborough Shoal standoff (2012–present) exemplifies this approach. Despite a clear 2016 ruling by the Permanent Court of Arbitration invalidating China's claims, Beijing has maintained de facto control of the reef without deploying warships. Instead, coast guard vessels and unmarked maritime militia operate in the area—asserting presence, intimidating Philippine fishermen, and bypassing formal conflict thresholds (Green et al., 2017). This slow-burn coercion, done without formal warfare, demonstrates how legal ambiguity becomes a strategic asset, enabling continuous pressure without triggering collective defense mechanisms or international intervention.

Similarly, Russia's shadow fleet, comprised of over 400–1,000 opaque oil tankers, illustrates another frontier of ambiguity. These vessels operate without active AIS (Automatic Identification System) tracking, under flags of convenience, and are now suspected of sabotage—such as the EstLink-2 power cable incident between Finland and Estonia in 2024 (Calero et al., 2025). These ships navigate a blurred zone between commerce and covert action, raising concerns about how state-linked actors exploit maritime deregulation for strategic disruption.

2. Use of Civilian Assets

Civilian platforms, particularly fishing vessels, research ships, and commercial tankers, are increasingly co-opted for state purposes, forming the soft edge of maritime power projection. Their very nature as "non-combatants" makes them politically and legally difficult to counter, creating dilemmas for targeted states bound by international humanitarian law and risk-averse diplomacy.

A well-documented case is China's People's Armed Forces Maritime Militia (PAFMM). In 2021, over 220 Chinese fishing vessels anchored in formation near Whitsun Reef, located in the Philippines' EEZ. While ostensibly engaged in fishing, satellite imagery revealed they were not fishing at all (Fillingham, 2024). Their coordinated presence, movement in formation, and persistent stationing suggested a well-orchestrated grey-zone campaign to assert sovereignty without triggering a military response. These vessels lack military designations but are state-directed, effectively turning civilian infrastructure into tactical leverage.

Even scientific missions are becoming dual-use. China's deployment of deep-sea research vessels like Xiangyanghong 16 in contested waters serves dual ends: while collecting oceanographic data under a civilian pretext, these ships gather strategic undersea mapping crucial for submarine operations and cable surveillance (Funaiole et al., 2024). Such operations blur the line between peaceful exploration and prepositioning for maritime dominance.

3. Information and Influence Operations

In hybrid warfare, perception is power. Control over the narrative surrounding maritime incidents often carries more strategic weight than the incident itself. State-linked media outlets, cyber trolls, and misinformation campaigns now serve as integral parts of maritime operations, shaping domestic opinion and diplomatic fallout in real time (Molander et al., 1996).

A striking example is India's deployment of INS Vikrant in April 2024 to the northern Arabian Sea. Indian news outlets, such as Mathrubhumi.com, headlined: "Pakistan's Nightmare! INS Vikrant's Battle Group Ready for Killer Blow." The sensational tone, amplified across social media, constructed a public narrative of dominance (Linganna, 2025). Yet, subsequent satellite imagery showed that the vessel returned to Karwar port after a brief deployment, influenced by persistent Pakistani naval patrolling. The disconnect between on-ground facts and media narratives reveals how perception warfare can be used to distract, posture, and test red lines without kinetic engagement.

Information operations also feed into strategic ambiguity. For instance, false flag incidents, such as unverified reports of aggressive maneuvers, can distort public discourse and create diplomatic paralysis. Such tactics make the information environment itself a battleground, where narrative superiority substitutes for firepower.

4. Cyber Operations

Maritime infrastructure is increasingly digitized, making ports, shipping networks, and naval communications vulnerable to non-kinetic but highly destructive cyberattacks. These attacks can paralyze critical logistics, cripple decision-making chains, and cause global economic ripples without a single shot fired (Shuja, 2025).

The 2017 NotPetya malware attack, initially targeting Ukraine, crippled Maersk, the world's largest container ship operator. Disabling operations across 600 ports worldwide, the attack inflicted $200–300 million in losses. NotPetya's effect was instantaneous and transnational, demonstrating how cyber sabotage can deliver strategic disruption rivaling conventional blockades (Wolff, 2021). A more insidious variation is cyber-kinetic warfare, where digital breaches cause physical consequences. The recent Lebanon pagers incident revealed how intercepted civilian communication systems (pagers) were manipulated to track sensitive supply chains. This shows how maritime hybrid threats now operate at the intersection of cyber surveillance, disinformation, and real-world logistics sabotage (Cohen & Shany, 2024).

Additionally, concerns have grown over dual-use tech platforms like Elon Musk's EstLink project, initially developed for Baltic data transmission. This initiative aims to shift the communication domain from the seabed to space (Mohydin, 2023). Intelligence analysts warn that such infrastructure, though commercially framed, could be exploited during crises to redirect digital flows or support clandestine communications,

highlighting the hybrid risks embedded in globally privatized maritime infrastructure.

5. Proxies and Non-State Actors: Violence with Distance

One of the most effective tools in hybrid maritime strategy is outsourcing risk through proxies. States increasingly rely on armed non-state actors to conduct operations that would otherwise trigger international condemnation or collective defense clauses.

The Iran-backed Houthi attacks on Saudi oil tankers in the Bab el-Mandeb Strait illustrate this perfectly. The use of remote-controlled explosive boats, sea mines, and short-range missiles allows Tehran to project deterrence without official involvement (Jones & Thompson, 2021). The 2018 attack on the Bahri tanker not only disrupted oil flows but also inflated shipping insurance and rerouted strategic cargo, a strategic gain achieved through tactical ambiguity (Wald, 2018). Private maritime security firms have also entered this space, often acting in legal twilight zones between military contractors and pirates. Their presence expands operational latitude and allows states to maintain distance from unlawful maritime activity while benefiting from its outcomes.

Implications of Maritime Hybrid Warfare

1. Hybrid maritime threats complicate deterrence by operating below the traditional threshold of armed conflict, making clear attribution difficult and legally actionable responses politically risky. When adversaries use unmarked vessels, maritime militias, or cyber proxies, conventional deterrence models collapse under ambiguity. States are placed in a strategic dilemma: respond decisively and risk escalation without legal certainty, or delay action and invite further coercion. This gray zone exploits gaps in collective security frameworks, such as NATO Article 5 or regional maritime agreements, where hybrid incidents may not legally qualify as acts of war, despite their strategic impact.

2. The increasing use of lawfare as a tactical instrument transforms international maritime law from a system of conflict resolution into a domain of conflict itself. States reinterpret UNCLOS provisions, manipulate EEZ designations, or invoke unverifiable historical rights to justify incursions and presence. This legal maneuvering enables strategic encroachment without firing a shot, placing the burden of legal counteraction on smaller or law-abiding nations. As law becomes a contested space, legal diplomacy, institutional preparedness, and rapid interpretive response become as vital to national maritime defense as physical deterrence.

3. Hybrid maritime warfare introduces a psychological dimension designed to erode confidence, both in state institutions and international alliances. By manipulating narratives through mainstream media and social platforms, adversaries create illusions of dominance, confusion about events, and fractures in public perception. The spectacle of naval deployment, even when tactically inconsequential, can influence diplomatic behavior and public opinion. This narrative warfare is calibrated not to escalate, but to induce strategic hesitation, delay decision-making, and create internal divisions among allies or within target states.

4. Civilian maritime infrastructure has become a primary vector for hybrid disruption. The 2017 NotPetya cyberattack that paralyzed Maersk's global shipping operations, and more recently, the suspected sabotage of EstLink-2, highlight how the maritime economy is now a frontline in conflict. These actions exploit the civilian-military duality of infrastructure, inflicting strategic damage without provoking formal war. States must now extend national security planning beyond the navy to include digital resilience, logistical redundancy, and public-private crisis coordination across the maritime sector.

5. The use of non-state proxies in maritime operations creates a legal vacuum where responsibility becomes difficult to assign, and rules of engagement become blurred. Proxy actors such as maritime militias or rebel groups like the Houthis allow state sponsors to project power while avoiding direct accountability. The ambiguity surrounding command and control relationships delays international response and weakens enforcement of maritime norms. This dynamic necessitates the development of new legal frameworks and intelligence-sharing mechanisms to close the accountability gap and respond proportionally to proxy-enabled maritime aggression.

Recommendations

States must reconceptualize maritime security from a platform-centric mindset to a systems-based approach,

treating the sea as a multi-layered arena of strategic, legal, cyber, and informational interaction. This includes viewing civilian maritime infrastructure, legal mechanisms, and perception management as equally critical components of national defense.

Adopting the MOSAIC warfare framework can help states restructure their maritime defense along modular, distributed, and rapidly reconfigurable lines. This means investing in interoperable units, manned-unmanned teaming, AI-assisted targeting, and decentralized operational cells. These forces must be trained to operate under ambiguous conditions and across kinetic and non-kinetic domains simultaneously, increasing resilience and reducing over-reliance on high-value, centralized platforms.

3. In an era where fishing boats may act as Q-ships, surveillance drones may fly under civilian registry, and research vessels may collect acoustic intelligence, hesitation can be catastrophic. Therefore, states must urgently review national laws and Rules of Engagement (ROE), especially for coast guards, port authorities, and maritime police units. Engagement rules must reflect the new grey zone where intent is ambiguous and attribution is delayed. Maritime actors should be equipped with pre-authorized response thresholds that allow for timely defensive action under unclear conditions.

4. Ports are now frontline targets in hybrid conflict, vulnerable not just to physical blockades but to digital sabotage. States should immediately strengthen cyber and port infrastructure by instituting mandatory cybersecurity baselines for all major ports. As every port has a physical security perimeter, it must now also have a "cyber wall" capable of defending against ransomware, GPS spoofing, malware infiltration, and network denial attacks. These cyber defenses should be complemented by redundant operational systems, offline backups, and emergency response drills.

5. States must boost their Maritime Domain Awareness (MDA) through AI-powered surveillance networks, satellite imaging, and multi-sensor data fusion. This requires real-time intelligence-sharing mechanisms, especially in chokepoints and disputed waters, and regional coordination platforms that can track anomalies and issue alerts before escalation occurs.

6. Hybrid attacks don't just hit navies, they strike at supply chains, telecom networks, oil infrastructure, and public morale. Therefore, states must organize whole-of-government and whole-of-society response that simulate complex maritime hybrid crises. Ministries of energy, transport, communications, foreign affairs, and the private sector must all be included in national preparedness strategies. Everyone must be part of the response net, including civil society and media platforms. National resilience is no longer built on firepower alone, but on cohesion, speed, and inter-agency reflexes.

7. As hybrid actors increasingly use lawfare to legitimize coercion, states must develop proactive legal capabilities to counter false claims and reinterpretations of international law. This includes training rapid-response legal cells capable of producing counter-claims, engaging international courts, and influencing global opinion in legal forums. Legal deterrence also means pre-registering territorial claims, filing early protests, and ensuring all national maritime boundaries are codified and defensible.

8. Given the complexity of hybrid attacks, traditional siloed responses are inadequate. States must establish Joint Hybrid Threat Response Units, integrating navy, cyber security agencies, legal strategists, and intelligence services into a single operational framework. These units must be empowered to make decisions quickly, escalate where necessary, and operate in both real-time and strategic domains.

9. No state can address hybrid maritime threats in isolation. Multilateral frameworks, such as ASEAN, IORA, or GCC, should develop regional hybrid security cells focused on maritime grey-zone dynamics. These should facilitate joint threat assessments, intelligence exchanges, legal coordination, and strategic foresight exercises. Standardized regional responses would significantly increase the cost of ambiguity for hybrid aggressors.

Conclusion

Hybrid threats, marked by ambiguity, legal manipulation, cyber disruption, and the use of civilian or proxy actors, have fundamentally altered the nature of maritime conflict. These threats operate below the threshold of conventional warfare, yet generate strategic outcomes by exploiting gaps in attribution, legal clarity, and institutional readiness. In this regard, the MOSAIC model offers a relevant and timely

framework to understand and respond to this complexity. Its emphasis on modularity, interoperability, and domain convergence aligns with the fluid, multi-layered nature of hybrid threats at sea. As demonstrated, contemporary maritime security requires a systemic approach, one that integrates legal, informational, cyber, and operational dimensions into a cohesive national and regional strategy. In conclusion, securing the maritime domain in the age of hybrid warfare necessitates a departure from platform-centric thinking and a shift toward systems-based resilience. States must institutionalize cross-domain coordination, legal agility, cyber preparedness, and anticipatory MDA to effectively deter and disrupt the mosaic of hybrid threats shaping the future of maritime conflict.

REFERENCES

Ball, J. (2023, April 15). What is Hybrid Warfare? Non-Linear Combat in the 21st Century. Global Security Review. Retrieved June 28, 2025, from https://globalsecurityreview.com/hybrid-and-non-linear-warfare-systematically-erases-the-divide-between-war-peace/

Bargués, P., & Bourekba, M. (n.d.). War by all means: the rise of hybrid warfare. CIDOB. Retrieved June 28, 2025, from https://www.cidob.org/en/publications/war-all-means-rise-hybrid-warfare

Bilal, A. (2021, November 30). NATO Review - Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. NATO. Retrieved June 28, 2025, from https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Calero, J., Olenska, A., & Kauranen, A. (2025, May 15). What is Russia's 'shadow fleet' of oil tankers? Reuters. Retrieved June 28, 2025, from https://www.reuters.com/markets/commodities/key-points-about-russias-shadow-fleet-oil-tankers-2025-05-15/

Clark, B., Pitt, D., & Schramm, H. (2020). MOSAIC WARFARE EXPLOITING ARTIFICIAL INTELLIGENCE AND AUTONOMOUS SYSTEMS TO IMPLEMENT DECISION-CENTRIC OPERATIONS. Centre for Strategic and Budgetary Assessment. https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf

Cohen, A., & Shany, Y. (2024, October 11). "Well, it Depends": The Explosive Pagers Attack Revisited - Lieber Institute West Point. Lieber Institute. Retrieved June 28, 2025, from https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/

Cullen, D. P. J. (2017). MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. In MCDC, UK.

DARPA Tiles Together a Vision of Mosaic Warfare. (n.d.). DARPA. Retrieved June 28, 2025, from https://www.darpa.mil/news/mosaic-warfare

Davidson, H. (2024, June 13). China's maritime militia: the shadowy armada whose existence Beijing rarely acknowledges. The Guardian. Retrieved June 28, 2025, from https://www.theguardian.com/world/article/2024/jun/13/china-maritime-militia-explainer-south-china-sea-scarborough-shoal

Debunking the Myth of 'Debt-trap Diplomacy' | 4. Sri Lanka and the BRI. (2020, August 19). Chatham House. Retrieved June 28, 2025, from https://www.chathamhouse.org/2020/08/debunking-myth-debt-trap-diplomacy/4-sri-lanka-and-bri

Deptula, D. A., & Penny, H. (2019). Mosaic Warfare. Air & Space Forces Magazine. Retrieved June 28, 2025, from https://www.airandspaceforces.com/article/mosaic-warfare/

Fillingham, Z. (2024, September 11). Backgrounder: The People's Armed Forces Maritime Militia (PAFMM). Geopolitical Monitor. Retrieved June 28, 2025, from https://www.geopoliticalmonitor.com/backgrounder-the-peoples-armed-forces-maritime-militia-pafmm/

Fridmen, O. (2018). The Birth of 'Hybrid Warfare'. In Russian "Hybrid Warfare": Resurgence and Politicization. Oxford Academic. https://doi.org/10.1093/oso/9780190877378.003.0003

Funaiole, M. P., Hart, B., & Powers, A. (2024, January 10). Surveying the Seas: China's Dual-Use Research Operations in the Indian Ocean. CSIS. Retrieved June 28, 2025, from https://features.csis.org/hiddenreach/china-indian-ocean-research-vessels/

Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017, May 22). Counter-Coercion Series: Scarborough Shoal Standoff | Asia Maritime Transparency Initiative. Asia Maritime Transparency Initiative. Retrieved June 28, 2025, from https://amti.csis.org/counter-co-scarborough-standoff/

Hawkin, c. (2017). Q-Boats and Chaos: Hybrid War on the High Seas. The Strategy Bridge. https://thestrategybridge.org/the-bridge/2017/12/7/q-boats-and-chaos-hybrid-war-on-the-high-seas

Hybrid warfare on the high seas - ICWA. (2025, February 26). Institute of Current World Affairs. Retrieved June 28, 2025, from https://www.icwa.org/norway-russia-arctic-hybrid-warfare/

Jensen, B. (2019, December 23). Mosaic Warfare: Small and Scalable are Beautiful – War on the Rocks. War on the Rocks. Retrieved June 28, 2025, from https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/

Jensen, B., & Peschkwitz, J. (2019, December 23). Mosaic Warfare: Small and Scalable are Beautiful – War on the Rocks. War on the Rocks. Retrieved June 28, 2025, from https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful/

Jones, S. G., & Thompson, J. (2021). The Iranian and Houthi War against Saudi Arabia. CSIS. https://www.csis.org/analysis/iranian-and-houthi-war-against-saudi-arabia

Korybokyo, A. (2015). Hybrid Wars: The Indirect Adaptive Approach To Regime Change Andrew. Institute of Strategic Studies and Predictions, Moscow, Russia.

Linganna, G. (2025, May 1). Pakistan's nightmare! INS Vikrant's Carrier Battle Group ready for killer blow. Mathrubhumi English. Retrieved June 28, 2025, from https://english.mathrubhumi.com/features/pakistan-ins-vikrant-carrier-battle-group-arabian-sea-karachi-firepower-enj0vtyo

McGowan, A. (2023, December 1). Mediterranean Tragedy: The Deadly Path to Europe's Shores. Think Global Health. Retrieved June 28, 2025, from https://www.thinkglobalhealth.org/article/mediterranean-tragedy-deadly-path-europes-shores

Mehmood, N., & Malik, A. I. (2021). Analysing Hybrid Warfare And Information/Cyber Operations. Webology, 18(4). https://shs.hal.science/halshs-03788137/document

Milestones in the History of U.S. Foreign Relations. (n.d.). Milestones in the History of U.S. Foreign Relations - Office of the Historian. Retrieved June 28, 2025, from https://history.state.gov/milestones/1866-1898/mahan

Missiroli, A. (2022). From Hybrid Warfare to "cybrid" Campaigns: the New Normal?. NATO Defence College. https://books.google.com.pk/books/about/From_Hybrid_Warfare_to_cybrid_Campaigns.html?id=zQ8y0AEACAAJ&redir_esc=y

Mohydin, R. (2023). The Politics of Dual-Use Technology: Starlink and the War in Ukraine. TRT World Research Center. https://researchcentre.trtworld.com/wp-content/uploads/2023/04/Starlink-UkraineV2.pdf

Molander, R. C., Riddile, A., & Wilson, P. A. (1996). Strategic Information Warfare: A New Face of War. RAND. Retrieved June 28, 2025, from https://www.rand.org/pubs/monograph_reports/MR661.html

Mumford, A., & Carlucci, P. (2022). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 192–206.

O'Donoughue, N. A., McBirney, S., & Persons, B. (2021, January 5). Distributed Kill Chains: Drawing Insights for Mosaic Warfare from the Immune System and from the Navy | RAND. RAND Corporation. Retrieved June 28, 2025, from https://www.rand.org/pubs/research_reports/RRA573-1.html

Orbaiceta, G. V. (2023). Close Encounters: China´s Little Blue Sailors and Hybrid Tactics at sea. IEEE, Ministry of Defence. https://www.ieee.es/Galerias/fichero/docs_opinion/2023/DIEEEO89_2023_GONVAZ_China_EN G.pdf a

Panda, A. (2018, March 25). China Condemns US FONOP Near Mischief Reef in the South China Sea. The Diplomat. Retrieved June 28, 2025, from https://thediplomat.com/2018/03/china-condemns-us-fonop-near-mischief-reef-in-the-south-china-sea/

Raydan, N. (2023, December 7). Houthi Ship Attacks Are Affecting Red Sea Trade Routes. The Washington Institute. Retrieved June 28, 2025, from https://www.washingtoninstitute.org/policy-analysis/houthi-ship-attacks-are-affecting-red-sea-trade-routes

Russia accused of jamming GPS navigation. (2024, May 2). BBC. Retrieved June 28, 2025, from https://www.bbc.com/news/articles/cne900k4wvjo

Shipping and World Trade: World Seaborne Trade. (n.d.). International Chamber of Shipping. Retrieved June 28, 2025, from https://www.ics-shipping.org/shipping-fact/shipping-and-world-trade-world-seaborne-trade/

Shuja, S. F. (2024, December 3). Beneath the surface: The strategic implications of seabed warfare | Opinion. Daily Sabah. Retrieved June 28, 2025, from https://www.dailysabah.com/opinion/op-ed/beneath-the-surface-the-strategic-implications-of-seabed-warfare

Shuja, S. F. (2025, May 19). The 5GW Playbook: Silent Wars and Invisible Battlefields. Global Security Review. Retrieved June 28, 2025, from https://globalsecurityreview.com/the-5gw-playbook-silent-wars-and-invisible-battlefields/

Soares, D. B. (2025, May 10). Understanding Maritime Disputes and Resolution Under UNCLOS. TATOLI Agência Noticiosa de Timor-Leste. Retrieved June 28, 2025, from https://en.tatoli.tl/2025/05/10/understanding-maritime-disputes-and-resolution-under-unclos/16/

STAVRIDIS, J. (2016, December). Maritime Hybrid Warfare Is Coming. Retrieved from US Naval Institute: Maritime Hybrid Warfare Is Coming Admiral James Stavridis, U.S.https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming

The Europan Hybrid Centre Of Excellence for Countering Hybrid Threats. (2019). Setting The Scene, Maritime Domain. In J. SAVOLAINEN, T. GILL, V. SCHATZ, L. OJALA, T. JAKSTAS, & P. KLEEMOLA JUNTUTEN, Handbook on Maritime Hybrid Threats (p. 13). Helsinki: The Europan Hybrid Centre Of Excellence for Countering Hybrid Threats.

The Europan Hybrid Centre Of Excellence for Countering Hybrid Threats. (2019). Legal Responses to Maritime Hybrid Scenarios. In J. SAVOLAINEN, T. GILL, V. SCHATZ, L. OJALA, T. JAKSTAS, & P. KLEEMOLA JUNTUTEN, Handbook on Maritime Hybrid Threats (p. 40). Helsinki: The Europan Hybrid Centre Of Excellence for Countering Hybrid Threats

STAVRIDIS, J. (2016, December). Maritime Hybrid Warfare Is Coming. Retrieved from US Naval Institute: Maritime Hybrid Warfare Is Coming Admiral James Stavridis, U.S.https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming

Tebel, R. (2023, March 10). Nord Stream Sabotage: The Evidence So Far. Geopolitical Monitor. Retrieved June 28, 2025, from https://www.geopoliticalmonitor.com/nord-stream-sabotage-the-evidence-so-far/

TZU, S. (500 BC). Attack by Stratagem page 8. In Art of War (p. 8)

Wald, E. R. (2018). Attack On Saudi Oil Tanker In Red Sea Prompts Halt To Oil Shipments. Forbes. https://www.forbes.com/sites/ellenrwald/2018/07/25/attack-on-saudi-oil-tanker-in-red-sea-prompts-halt-to-oil-shipments/

White, black or red, Coast Guard needs new hulls – Professional Mariner. (2021, March 1). Professional Mariner. Retrieved June 28, 2025, from https://professionalmariner.com/white-black-or-red-coast-guard-needs-new-hulls/

Wither, J. K. (2020). Defining Hybrid Warfare. Concordium, George C., Marshal Center of Securiyt. https://www.marshallcenter.org/sites/default/files/files/2020-05/pC_V10N1_en_Wither.pdf

Wolff, J. (2021). How the NotPetya attack is reshaping cyber insurance. Brookings. https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/.