

Critical threats in the maritime domain. The role of cutting-edge technology in a conflict and Digital: The New Type of War.

Dimitrios Tsailas (ret) Admiral)

(He has taught for many years, operational planning, strategy, and security, to senior officers at the Supreme Joint War College. He is a member and researcher of the Institute for National and International Security)

Copyright: @ 2025 Research Institute for European and American Studies (www.rieas.gr) Publication date: 1 June 2025

Note: The article reflects the opinion of the author and not necessarily the views of the Research Institute for European and American Studies

Imagine a silent vessel drifting through a calm-gray sea. Its radar registers nothing unusual. The crew goes about its duties. But 200 meters below, a data cable pulses with the heartbeat of global communication. Above, a drone observes. And onshore, an algorithm has already decided this ship's risk level.

This isn't a scary film. It's the new face of maritime reality. In today's world, war doesn't always arrive with cannon fire. It arrives in signals, in shadows, in silence.

The maritime domain has become the silent frontier of digital conflict—a place where traditional threats like piracy, terrorism, and smuggling blend with cyber warfare, state manipulation, and environmental sabotage.

Today, we navigate the key threats to our oceans, the role of cutting-edge technology, and why the digital sea may be the most dangerous front of all.

Cutting-edge technology creates comprehensive and reliable war deterrence. Navigating the Future of Conflict at Sea

“There will be other ways and means that no one can currently foresee, since war is certainly not one of those things that follows a fixed pattern. On the contrary, it usually creates its own conditions to which one must adapt in the face of changing situations.”

— Thucydides

The optimal strategy is the one that counterbalances today's multiple threats and prevents the wars of tomorrow. With this in mind, however, the level of ambition and expectations from the Armed Forces increases, as they will be required—due to the multiplicity of threats—not only to confront them but also to deter them. The issue that arises with such an approach is that in choosing to do everything, priorities are

lost. Inevitably, this will result in a failed approach against the most difficult and complex risk management threats.

Although this approach may sound like a good way to protect against future uncertainty, it can lead to a military force unable to reliably defend against any given attack. Historically, the need to build and maintain a large, battle-ready military force has often displaced modernization (as was the case with the Soviet army during the Cold War). Armed forces clearly need both sufficient personnel and capability in new weapon system technologies, but inevitably, a trade-off exists between these two if resources are limited. Today, this tension is even greater as military personnel and the costs of operational readiness and maintenance consume an even larger share of the defense budget, leaving a smaller portion available for modernization.

Nevertheless, additional resources alone will not resolve this dilemma. If extra funding is used to acquire weapon systems with greater capabilities that do not align with high-standard deterrence, the problem may worsen over time and further reinforce resistance to the necessary changes.

Warfare in the 21st century will prove to be a constantly shifting and dynamic environment, unlike anything previously known in the history of combat readiness—deploying military forces across all theaters of operation critical to national interests. The shared objective and core issue that must be solved by the entire military hierarchy is to successfully conduct warfare across all known domains through the implementation of network-centric operations. For the Navy, this is no different. As the Navy continues to evolve, adapt, and redesign itself in response to these new challenges, it must not overlook its warfighting philosophy. Instead, it should embrace concepts such as maneuver warfare that have made it a successful combat force for centuries, while also evolving its doctrines. Thus, the Navy continues to train and implement new doctrines, with a focus on modern equipment and technology to conduct simultaneous, combined defense operations across all five domains of warfare (surface, anti-air, anti-submarine, cyber, and space). In this way, it will prove tactically effective on the battlefield of the future.

With the new Fleet architecture, deterrence is applied through a focus on the information technology revolution, aiming to enable the capability to rapidly collect and assess vast amounts of information about any data point within the operational theater—at long distances and under protection. For technology visionaries, sensor systems, data processing centers, and digital communications are the speed and decision-making advantage necessary for victory. Beyond speed and decision advantage, persistence and resilience are two more key components. With this in mind, the armed forces should focus on building decentralized networks, invest in tactics that reduce the economic cost of war, and develop weapon systems and strategies that degrade the effectiveness of threats.

What the armed forces now require is a new theory of victory for an environment in which information and the networks through which it flows are under threat. I assess that victory will be achieved through information technology, enhancing situational awareness so that combatants can strike from greater distances, respond more rapidly to threats, and target more accurately. Consequently,

investments in technology primarily enhance efficiency and speed while providing an advantage in security and resilience. According to this theory, decentralized and efficiency-optimized networks, along with weapon systems that are not simply data-enabled but data-dependent, can deliver swift and decisive strikes.

The acquisition of new Frigates and Corvettes, in conjunction with new aircraft, begins with a better understanding of how networks survive under threat. These networks rely on speed in collecting, storing, and analyzing data from various sources, integrating them through gateways between users. This kind of "network-centric warfare" allows for the merger of data with artificial intelligence while reducing unnecessary information and minimizing access points that could create cybersecurity vulnerabilities.

With this mindset, we are also allowed to change how we approach the cost of war. The economic cost has been largely absent from military discussions, which have instead focused on the need to avoid casualties that would undermine the public support for wars. Network-centric operations solve the problem of political will by using technology as a means of force protection.

Finally, deterrence will come from the ability to persist over time—not merely to dominate in a single moment—as this is what will ultimately deter adversaries from initiating the first attacks. Until now, military reforms have not been about chasing the next technology; they have always involved experimentation and responsiveness. It is time for the armed forces to adapt to the next-generation cutting-edge technologies—not merely upgrade to the latest version of already outdated systems.

In this vulnerable global order of a maritime century defined by unprecedented dependence on the seas for sustainable prosperity, I believe it is time to redefine naval operations, moving away from the approach originally articulated during the previous era of warfare. I argue that this is precisely why we need an analytical shift aimed at redesigning what navies do, using modern methods, within a broader context. The objective must be reformulated because what navies do have a unique strategic value that cannot be reproduced elsewhere within a national military mechanism.

At that moment, I will attempt a rapid assessment of what the future holds for warfare in the Red Sea. By analyzing the factors and conditions using the method of rapid situation assessment, we identify the nature of a limited yet consequential maritime conflict. Always, the first, supreme, and most comprehensive act of crisis analysis is to determine the kind of war in which the belligerents are engaged. We must be clear. We must neither confuse it nor attempt to transform it into something alien to its nature. This is the first of all strategic questions—and the most complete—that we must answer.

We then analyze the factors and conditions of this war. From this analysis, we can distinguish four defining factors of this limited conflict:

First, we see an irregular land-based paramilitary group employing military-grade equipment in unconventional operations, opposing actors who are deploying conventional naval forces against them. The naval coalition protecting commercial

shipping faces yet another unconventional war that blurs the boundaries between irregular and conventional methods of warfare.

Second, both the Houthis and the coalition naval forces (e.g., Operation Aspides, aimed at securing freedom of navigation) are waging a limited war against each other. Unlimited war implies the violent overthrow of a hostile government and the imposition of one's will upon the defeated. The Yemeni insurgents neither possess the means nor express the intention to overthrow any government; they claim their operations are acts of solidarity with the Palestinian cause. Their goal is merely to harm Israel and the naval forces supporting Israeli operations in Gaza. This inflicts economic pain and raises the operational cost for the coalition. From the Western side, the elimination of the Houthis has not been declared as an objective. Their aim is simply to deter attacks on shipping so that normal maritime trade patterns can resume—i.e., a limited objective: restoring the status quo of safe sea lanes. The problem arises when it becomes clear that halting the Houthi attacks may require the destruction of their armed groups. But that could mean embracing unlimited objectives—requiring military escalation.

Third, there is a mismatch between how much we desire to achieve our objectives and how many resources we are willing to expend to achieve them. As Clausewitz notes, the value placed on the political object—the goal of a warlike endeavor—determines the amount of resources and the duration of the effort. Size equals the rate at which a belligerent expends military-related resources; duration is how long they continue to do so. (Clausewitz's equation: Resources \times Time = Cost of Political Objective). If political leaders, society, and armed forces have the will and the means to pay the price, the campaign continues. If not, they withdraw.

In analyzing the conflict in the Red Sea, we find that religion (Islamism) is a significant driver in the political and strategic calculations of the Houthis. It motivates their militant leaders to place great importance on their political objectives. In other words, the will of the Houthis to achieve their objectives in the Red Sea dictates both the rate at which they are willing to expend military resources and the length of time they are prepared to continue doing so. Because it is crucial for the Houthi leadership to proclaim success for Gaza, they are willing to exhaust all available military supplies, for as long as needed, to amplify that message. This signals a prolonged campaign against maritime traffic.

On the other hand, it is not clear that Western defenders of maritime freedom place as much value on their objectives in the Red Sea as the Houthis do on theirs. Prosperity is threatened in other “marginal maritime zones” across the Eurasian periphery—not only in the Red Sea but also in the Black Sea, Eastern Mediterranean, Arabian Sea, and South China Sea. The freedom of navigation—of ships sailing from one port to another—is under threat.

Fourth, both the Houthis and participants in Operation Aspides are conducting cumulative unconventional operations. These campaigns, by nature, are ineffective in producing decisive outcomes—but that does not matter for the Houthis. It matters greatly for coalition naval forces, which require decisive outcomes to prevail. Unlike what the Houthis are doing, sequential operations are the norm in military history: a

campaign progresses from one tactical action to the next until the strategic goal is reached. Each action builds on the previous one and shapes the next. Only sequential operations can deliver decisive results and control—whether of geographic space, enemy forces, or other strategic objectives.

By contrast, cumulative operations consist of isolated tactical actions that do not follow one another in a coordinated temporal or territorial sequence. A belligerent pursuing a cumulative strategy seeks to wear down the opponent by inflicting low-grade damage via asymmetric attacks rather than through a deliberate sequence of retaliatory blows aimed at victory. Air and missile strikes like those being executed are essentially cumulative in strategy. In this way, the Yemeni insurgents aim to achieve their goals without a decisive outcome. They do not need to sink all coalition shipping—just spread enough chaos to keep shipping insurance premiums high, discourage transit through the Red Sea, or impose a significant cost on those who dare attempt the journey. In short, they seek to inflict an economic headache on the commercial world. A sporadic missile or drone attack is sufficient for their purposes.

On the contrary, coalition warships and aircraft require a decisive outcome. They must completely neutralize the Houthi threat to restore trust in maritime security and allow global trade to resume. However, the current analysis suggests they are conducting an inherently ineffective campaign.

Having examined the conflict's key factors, we now turn to its conditions:

The Houthis have been at war, launching missiles into the Arabian Peninsula since 2015, indicating they possess a considerable arsenal. They enjoy Iranian backing—including maritime arms shipments—and exploit weapons seized from Yemen's regular armed forces during the civil war. They have also proven adept at repurposing older weaponry for maritime missions. Despite being a U.S. ally with advanced American weaponry, Saudi Arabia has proven incapable of fully suppressing cross-border Houthi attacks on its infrastructure, even with the deployment of modern Western anti-air systems.

We know that in unconventional warfare, insurgents can replenish their expenditures and losses through Iranian resupply or their own weapon manufacturing. They do not need much. A low-level asymmetric campaign is enough to wreak havoc. Since their goal is to remain a disruptive force, creating chaos is easy.

On the other hand, the goal of stopping those who seek chaos imposes a terrifying standard of success: total elimination of all threats to Red Sea lanes—a nearly impossible benchmark for the coalition navies. Frustration is inevitable if the coalition persists with the current cumulative strategy without shifting to a sequential strategy that could produce previously unthinkable victories. Yet sequential operations would likely mean deploying troops on land—another ground war in the Middle East—at a time when the West needs to focus its attention and resources on other flashpoints across the globe.

The world wonders: What is the endgame in this low-grade maritime war in the Red Sea—and when will we get there?

My answer: Don't hold your breath.

For the Yemeni Houthis to no longer be a threat to shipping, the Western naval coalition must completely defeat the Houthi threat to reestablish freedom of navigation. Coalition leaders are likely to remain silent about what that truly entails. And if they don't, yet proceed anyway, then another ground war in Yemen awaits. Ground campaigns in the Middle East rarely end quickly—or cleanly. Regardless, the signs point to an extended, indeterminate struggle between coast and sea.

The Role of Cutting-Edge Technology in a Conflict

Definitely, a military conflict would be catastrophic, and every effort must be made to prevent such an outcome through all available means—diplomatic and military. However, continuous preparation is necessary, demanding, and critical for defense planners in a way that prioritizes the strengthening and modernization of the forces, while also identifying potential shortcomings in the design and readiness of the Armed Forces.

In today's environment, where new forms of warfare dominate, cutting-edge technology is the main factor that will significantly enhance the military capabilities of the opposing sides. Investments in technology prioritize short-term offensive capabilities. In particular, cyber warfare could play a major role in the Armed Forces' efforts to disrupt and downgrade the opponent's battle network and compensate for domestic shortcomings in submarine warfare and the electromagnetic domain. Meanwhile, air-naval reinforcements could enhance operational readiness and capacity through joint-force cooperation, contributing to a strong deterrent defense.

Technology as the New Strategic Center of Gravity

The decisive edge in future conflicts will not be defined solely by troop numbers or conventional firepower, but by technological supremacy—particularly in cyber warfare, electromagnetic operations, and AI-enhanced systems. Defense investments must therefore prioritize short-cycle, high-impact capabilities that enable rapid adaptation and cross-domain superiority.

Cyber operations are poised to play a central role in this transformation. By targeting and degrading adversary command-and-control systems, cyber tools can offset asymmetries in conventional domains. This is especially critical for nations seeking to neutralize superior naval or aerial assets through precision disruption rather than direct confrontation.

Moreover, integrated joint-force structures—especially in air and maritime domains—are essential for maximizing operational readiness. When supported by real-time data fusion and AI-enhanced coordination, they become formidable instruments of deterrence and, if necessary, decisive response.

Unmanned Systems and the Rise of the Autonomous Battlespace

In the initial phases of conflict, we must expect a multidimensional information warfare campaign. This will likely include AI-generated disinformation aimed at shaping global narratives, undermining political cohesion, and delegitimizing defensive measures. Controlling the information domain will be as crucial as physical battlefield dominance.

Once hostilities commence, critical infrastructure—sensors, satellites, and communication actions—will become high-value targets. In this context, the role of **unmanned aerial vehicles (UAVs)** and **autonomous systems** cannot be overstated. Swarms of UAVs, equipped with radar-jamming equipment and AI navigation, can overwhelm even sophisticated air defense networks. Deployed strategically, they serve as both reconnaissance and denial assets.

In the maritime domain, we anticipate the deployment of expansive underwater sensor networks and autonomous sub-surface vehicles. Powered by machine learning and big data analytics, these systems can detect, classify, and relay submarine movements, dramatically enhancing situational awareness and mitigating anti-submarine warfare vulnerabilities.

Strategic Implications and Policy Imperatives

The convergence of artificial intelligence, unmanned systems, and cyber-electromagnetic operations marks a pivotal evolution in military doctrine. This is not a future projection—it is a current operational reality. Our response must be holistic, forward-thinking, and clear by legacy assumptions.

For military leaders, the challenge lies in integrating these technologies not as isolated assets but as part of a unified, adaptive warfighting architecture. For policymakers, it is essential to provide the frameworks, funding, and strategic clarity required to accelerate development and integration. And for academics, the imperative is to explore these transformations critically, identifying ethical boundaries, doctrinal shifts, and potential escalatory risks.

In sum, technological edge is no longer a supplementary advantage—it is the strategic basis upon which modern deterrence and defense rest. Our readiness to embrace and operationalize this truth will define not only our military posture but our geopolitical future.

Digital: The New Type of 6th Generation Warfare

The winner will be the side that most quickly understands how to exploit the capabilities of digital warfare.

The reform of the Armed Forces has been part of an ongoing discussion since the early 2010s. However, the focus of this discussion should have been primarily on the characteristics of modern warfare and the type of war we need to prepare for. Simply put, two interrelated models of contemporary warfare should have been at the forefront of this dialogue.

The first is the "new type of war." This refers to warfare based on a holistic understanding of modern conflict. In the initial, non-military phases of confrontation, the goal is to weaken the opponent through "active measures" such as disinformation and destabilization—essentially, psychological warfare—through cyberattacks. Once conflict shifts into the military phase, not only regular troops are used, but also irregular violent actors operating in close coordination with military leadership. Therefore, there is a need to build a substantial reservoir of such so-called proxies.

The second guiding principle of military reform should be the concept of "6th generation warfare," also known as "five-dimensional network-centric warfare." These five dimensions are: underwater, surface, aerial, space, and cyberspace. These principles should also dominate discussions about the final military stages of the new type of war. Behind this lies the idea of network-centric warfare: that future military operations will be conducted over great distances (beyond the horizon), primarily using advanced networked systems and sensors operating in the air and space. In simple terms, it is a digital war.

Two key traits define this digital war. First, the flood of unclassified information and interceptions helps intelligence services gain an accurate picture of the situation, but can also lead to confusion and baseless bias. Second, it is not focused on combat capabilities based on advanced technology alone, but highlights the dynamic arena of the digital space, operating near—or sometimes within—the battlefield, involving millions of individuals connected to the internet.

The Art of Information Gathering and Analysis

Evaluating information is like trying to complete a puzzle. The art of intelligence services lies in placing the existing pieces correctly and imagining how the missing ones might look to envision the whole picture—based on in-depth knowledge of the enemy, research methodology, and data collection capabilities.

The flood of unclassified information and interceptions changes the rules of the game by supplying many of the missing puzzle pieces—especially in extreme scenarios like war. In the war in Ukraine, unclassified data filled huge gaps in understanding combat situations and provided more accurate and reliable answers than any other source regarding the extent of the damage. This is a crucial example, as these are the questions decision-makers worldwide must answer when planning actions and determining levels of support.

At the same time, using information—especially open-source—to make decisions carries risks. In the puzzle metaphor, more pieces than necessary can distort the image, framing it in a misleading and fundamentally different way. While this can foster creativity and imaginative expansion in some contexts, in wartime, intelligence personnel need tools that help them focus and avoid confusion or bias. Today, there's clearly more information available than needed—and more room for interpretations that could mislead decision-makers. Open-source intelligence alone is not enough.

A Paradigm Shift in Intelligence Work

A significant shift is now evident: while in the past, military intelligence tended to restrict information gathering to open domains and rely primarily on classified sources, today such an approach would be irresponsible. It would ignore the wealth of accessible and valuable information and, more critically, disregard a key arena of modern warfare.

What are the lessons from the war in Ukraine regarding the proper use of information in times of war?

The mission of intelligence services is to gather as much enemy information as possible and dispel the fog of war. Today, in the open realm of the internet and mass media, we can find satellite photos of the battlefield, technical system data collected by media companies (location, activity patterns), and a wealth of content gathered and shared on social media and news outlets. Much of the intelligence used by Ukraine before and during the Russian military invasion was acquired this way. Since this information was largely unclassified, it could be analyzed using advanced AI-based processing capabilities developed by private tech giants. The processed data was easily shared with intelligence services globally—and especially with Ukraine—without the political barriers that normally complicate the work of secret agents.

Thanks to this capability, the fog of war in the current conflict in Ukraine has been remarkably absent—due to the immense volume of open-source information being transmitted in real time online from the battlefield. We see how the use of open-source intelligence, drawing on social media analysis communities and AI tools (including those from private entities), has enhanced the Ukrainian military's ability to gather intelligence and compensate for Russia's relative advantage. Continuous international support, particularly in intelligence—but also in military and economic terms—has also been a vital factor.

The Information War and the Battle Against Deception

Information warfare and deception are well-known elements of military doctrine. Today, intelligence services increasingly shoulder the responsibility of systematically countering disinformation. One of the critical capabilities in digital warfare is superiority on social media and digital platforms—measured by the ability to grasp public sentiment, issue real-time reports, and debunk rumors using credible sources.

In Ukraine, there was extensive use of public messaging to reveal the course and outcomes of battles—sometimes strategically deployed in opposing propaganda campaigns. It is evident that the Ukrainian military and civilian use of open media led to a more accurate perception of reality.

Intelligence services are aware of both the benefits and pitfalls of open-source information. The dramatic progress in the field has led to global revelations about the capabilities of intelligence gathering and AI-driven analysis. As a result, military mobilization today still demands secrecy and careful coordination—particularly in avoiding signal transmissions.

A New Relationship Between the State and the Digital World

The relationship between the state, the Armed Forces, and intelligence services on one side—and social media, private platforms, and the public on the other—must be one of mutual respect and rules. Compared to Ukraine’s experience, it is doubtful whether Western countries are ready to utilize public and private companies effectively. Yet if we do not adopt this new approach now, we will likely be unprepared for the challenges ahead.

The core purpose of intelligence is to support decision-makers, helping them craft policies in response to evolving situations, and to guide operational agencies on how to prepare, maintaining political, economic, and military advantages. However, in recent years—due to radical changes in the information and media landscape, and the rising power of social media and global public opinion—espionage itself has become a tool for policy implementation and influence.

The case study of public information use in the Ukraine crisis, along with the accumulated insights, offers a valuable perspective, clarifying both the advantages and limitations and the costs and benefits of this increasingly common practice in international affairs.

Conclusion

So, where does that leave us?

The ocean has always been a place of mystery, of promise. But now, it’s also a zone of fragile peace. The calm surface hides layers of risk—from pirates with laptops to nations with reliable deniability.

We must reimagine maritime security—not just in terms of navies and borders, but in data integrity, ecological balance, and global coordination.

Because in the new digital war, the frontlines are invisible.

And as technology shapes conflict, ethics must shape our response.

Let me leave you with this:

The sea does not speak. But it remembers. And if we fail to listen, it's silence may become our storm.