

All-Domain Irregular Warfare:

A Framework for Modern Strategic Competition

Article by **Sal Artiaga**

October 29, 2025



Introduction

In the modern strategic environment, conflict rarely fits neatly into the mold of conventional warfare. The United States recognizes five operational domains: land, maritime, air, space, and cyberspace, each representing a distinct arena where military competition unfolds. But as the world moves deeper into an era of strategic competition, the boundaries between these domains have blurred, especially when adversaries use irregular methods to achieve political aims without resorting to open war. This convergence has given rise to what can be described as **All-Domain Irregular Warfare (ADIW)**, a deliberate fusion of irregular activities across every domain to pressure, influence, and erode an opponent's resolve in the "gray zone." Unlike traditional irregular warfare, which historically emphasized guerrilla tactics, insurgency, and proxy conflict, ADIW operates in a fully integrated, multi-domain environment, exploiting every available tool from disinformation to cyberattacks, economic coercion, proxy conflict, and legal manipulation.

Distinguishing ADIW from Hybrid Warfare

The difference between ADIW and hybrid warfare is key. Hybrid warfare merges traditional military strength and irregular methods, so a country, for example, marshals its own standing army together with proxy militias, domestically capable. Russia did just that in Crimea in 2014.

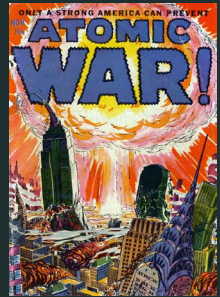
On the other hand, ADIW is an entirely irregular form of warfare held below thresholds. Conventional forces are not the main instruments; here, instead, emphasis is on integrating this kind of irregular action across all domains to produce strategic effects without triggering large-scale armed conflict. Certainly not least, the difference is not only theoretical, but it also causes genuine concern. Recognition of this will assist in formulating effective counter-measures. Where hybrid warfare escalates toward kinetic conflict, ADIW thrives on never crossing that line.

Historical Roots of Multi-Domain Pressure

Although the term “All-Domain Irregular Warfare” is new, the strategic logic behind it has deep historical roots. During the Cold War, both the United States and the Soviet Union waged complex campaigns that blended propaganda, espionage, proxy wars, and economic pressure, early forms of multi-domain competition before “space” and “cyberspace” were recognized as warfighting domains.

From the Soviet use of “active measures” to undermine Western cohesion, to U.S. efforts supporting anti-communist resistance movements worldwide, the essence of

ADIW, applying pressure simultaneously across different arenas, was already present. Today, technology has expanded the number of domains available, but the principle remains the same: **win without a decisive battle.**



The Current Joint Definition of Warfare

U.S. Joint Doctrine defines warfare as the conduct of military activities, both lethal and nonlethal, undertaken to achieve political objectives. This broad definition is flexible enough to encompass irregular strategies conducted below the threshold of war. In doctrinal terms, the U.S. military considers five domains of warfare: land, maritime, air, space, and cyberspace.

While doctrine often treats them as separate arenas, in ADIW they become fully interconnected and mutually reinforcing, producing effects that are greater than the sum of their parts. The result is a form of competition that is not just multi-domain but omni-domain, where the adversary can apply simultaneous pressure everywhere without triggering conventional escalation.

Applying All Domains to Irregular Warfare

The essence of ADIW lies in integration and synchronization. In the land domain, adversaries infiltrate political systems, co-opt social movements, and sabotage infrastructure without deploying formal armies.

At sea, they use maritime militias and coast guard incursions to undermine sovereignty without naval battles. In the air, constant incursions exhaust readiness and create psychological strain. In space, adversaries disrupt satellite operations and jam communications. In cyberspace, they run influence campaigns, steal intellectual property, and erode trust in government institutions. None of these actions are isolated, they are designed to work together, amplifying each other's effects in a coordinated campaign.

A Case Study in ADIW

Taiwan is the most obvious real-world demonstration of ADIW. China's campaign is relentless and multi-layered. Ashore, it subsidizes friendly media and builds political surrogates and insinuates itself within social movements.

Afloat, Chinese maritime militia and coast guard ships edge into Taiwan's waters, testing the way the Taiwanese respond without going to war.

In the air, PLA planes make near-daily incursions into Taiwan's ADIZ, necessitating constant alertness. Chinese satellites in orbit deliver intelligence to guide other operations.



Waves of intrusion and propaganda attacks bombard Taiwan's government and financial infrastructure in cyberspace, often coordinated in an effort to have the greatest political impact.

Every move is calculated, integrated, and designed to erode Taiwan's will to resist without provoking U.S. military intervention.

Institutional Barriers to Countering ADIW

Countering ADIW requires more than recognition, it demands overcoming the structural weaknesses of the U.S. government.

The greatest challenge is not capability, but coordination. The Department of Defense, State Department, Treasury, and Intelligence Community each have their own cultures, authorities, and budgets, leading to "siloed" approaches. While military doctrine speaks of "unity of effort," in practice the U.S. often settles for unity of purpose, agreement in principle without the mechanisms for joint execution. Adversaries like China and Russia exploit these seams, knowing that America's bureaucratic fragmentation slows decision-making. Without a structural solution to integrate interagency planning and operations, the U.S. risks being perpetually reactive.





Defining All-Domain Irregular Warfare

To be operationally useful, ADIW can be defined as:

“The integrated use of irregular methods across all warfighting domains, land, maritime, air, space, and cyberspace, to achieve political objectives below the threshold of armed conflict, exploiting legal, informational, and operational vulnerabilities to erode an adversary’s will, legitimacy, and freedom of action.”

This definition emphasizes two points: integration across all domains, and the deliberate decision to stay below the war threshold. It also reinforces that ADIW is not simply another name for hybrid warfare, it is a strategic discipline focused on long-term pressure without decisive battles.

Why This Matters for U.S. Strategy

Recognizing ADIW changes how threats must be assessed and countered. In the past, cyberattacks, maritime harassment, and political interference were treated as separate incidents; ADIW forces us to see them as parts of a single, coordinated campaign. The U.S. must break down interagency silos, align authorities, and adopt persistent engagement across all domains. Equally important is building resilience in partners like Taiwan, not just through military aid, but through economic security, cyber defense, and social cohesion.



Conclusion

All-Domain Irregular Warfare is the logical evolution of gray-zone competition, a synchronized, multi-domain pressure campaign that blends the subtlety of influence operations with the reach of modern technology. Taiwan's experience shows how devastatingly effective ADIW can be when executed with patience and precision. Countering it requires the U.S. to do more than have unity of purpose; it requires true unity of effort, breaking down institutional silos to integrate the capabilities of the entire national security apparatus. Without that integration, the United States risks preparing for yesterday's wars while losing today's all-domain fight.

M6

