Beyond Missiles and Marines: A Multidomain Strategy for Deterring a PRC Invasion of Taiwan

Timothy Shives and Rose Kingham
Naval Postgraduate School, Monterey, California, USA

timothy.shives@nps.edu
rose.kingham@nps.edu

Abstract: The People's Republic of China (PRC) poses a critical challenge to regional stability and U.S. security interests, advancing a strategy of Unrestricted Warfare that outpaces traditional battlefield engagements. A Taiwan crisis may unfold through cyberattacks, economic coercion, and disinformation designed to fracture alliances and erode public trust long before the first missiles are launched. If U.S. deterrence remains narrowly focused on kinetic superiority, it risks failing to leverage an Inverse Unrestricted Warfare Framework which—combined with *U.S. Marine Corps Force Design 2030 (commonly referred to as "Force Design")*—offers a multidomain approach that mirrors and counters the PRC's own tactics. This paper proposes a multidomain strategy to deter a PRC invasion of Taiwan through a cohesive framework that applies the logic of Unrestricted Warfare against the PRC itself. The framework consists of five mutually reinforcing lines of effort: Military Denial Through Distributed Operations; Non-Kinetic Domain Deterrence; Cognitive and Informational Maneuver; Asymmetric Disruption and Escalation Options; and an Integrative Principle of Preemptive and Parallel Shaping. Beyond kinetic means, the framework emphasizes cyber resilience, legal warfare, and economic pressure as critical tools for shaping the pre-invasion battlespace. The result is a layered deterrence strategy that combines denial, cost imposition, and delegitimization, leveraging the PRC's own tactics against it to impose strategic costs. An Inverse Unrestricted Warfare framework integrates military innovation with non-kinetic resilience, ensuring *Force Design* enables deterrence that is credible, adaptive, and global—preventing conflict before it begins and safeguarding Taiwan's future.

Keywords*:* Unrestricted warfare, Gray zone conflict, Taiwan deterrence strategy, Marine Corps Force Design 2030, Multidomain deterrence and distributed operations, Cognitive and information warfare, Non-kinetic deterrence

1. Introduction

The People's Republic of China (PRC) may ignite a war over Taiwan without firing a single shot, employing the principles of Unrestricted Warfare first articulated by People's Liberation Army (PLA) colonels Qiao Liang and Wang Xiangsui. Their concept reframed conflict as an activity unconstrained by traditional military domains, extending competition into political, economic, technological, and informational arenas. Rather than seeking immediate battlefield victory, the PRC seeks to shape strategic conditions, exploit ambiguity, and constrain adversary decision-making before leaders recognize that competition has already crossed into conflict (Qiao & Wang, 1999).

This approach is evident in the PRC's persistent use of gray zone tactics—actions that fall between total war and perfect peace. These tactics include cyber intrusions, economic coercion, legal manipulation, and influence operations designed to weaken political resolve and delay coordinated response (Braw, 2022). In the Taiwan context, a crisis is unlikely to begin with amphibious assault or missile strikes. Instead, it may open with infrastructure disruptions, financial instability, and coordinated disinformation intended to erode confidence in governance and alliance credibility.

Current U.S. deterrence frameworks remain disproportionately oriented toward kinetic superiority, assuming that military denial alone will prevent aggression (Braw, 2022). This assumption is increasingly risky. If deterrence activates only when overt military indicators appear, the PRC may already have achieved decisive advantage by shaping perceptions, degrading command and control, and narrowing political options through non-kinetic means. Deterrence that arrives late—after strategic conditions are already set—may prove ineffective even if conventional forces remain capable (Schneider Rasador and Moreira Cunha, 2025).

The PRC's approach deliberately targets structural vulnerabilities within U.S. and allied systems, including centralized logistics, fragile information flows, and alliance coordination mechanisms. These vulnerabilities are magnified by decision latency, interoperability challenges, and policy constraints that slow integration across partners and domains (Zheng, 2025). In a rapidly unfolding Taiwan contingency, such friction could delay collective action and create opportunities for coercion to succeed without decisive military engagement.

The U.S. Marine Corps is uniquely positioned to address this challenge through the concepts embodied in *U.S. Marine Corps Force Design 2030 (commonly referred to as "Force Design")*. Emphasizing distributed operations, expeditionary resilience, and integration across domains, *Force Design* provides the foundation for a deterrence

posture capable of competing inside the gray zone. By combining distributed military denial with cyber resilience, legal and economic instruments, and cognitive maneuver, the Marine Corps can contribute to a deterrence strategy that operates before conflict becomes inevitable.

This paper advances the concept of an Inverse Unrestricted Warfare framework—a multidomain approach that turns the logic of Unrestricted Warfare back against the PRC. Rather than responding sequentially to coercive actions, this framework seeks to shape the shaping fight through parallel, preemptive actions across military and non-military domains. The objective is not escalation, but prevention: creating a deterrence posture that denies the PRC the ability to achieve strategic objectives through ambiguity, timing, and coercion.

2. Problem

The central problem addressed in this paper is that U.S. deterrence concepts remain optimized for kinetic conflict, while the People's Republic of China (PRC) has invested heavily in shaping the pre-conflict environment through gray zone methods that exploit ambiguity and delay response (Qiao & Wang, 1999). In a Taiwan contingency, deterrence failure may not stem from an inability to win a conventional fight, but from the failure to recognize that strategic competition has already transitioned into conflict across political, informational, economic, and cyber domains (Zheng, 2025).

The PRC's strategy of Unrestricted Warfare enables it to pursue national objectives without crossing clear thresholds that would trigger immediate military response. By integrating cyber operations, economic pressure, legal manipulation, and information campaigns, Beijing can impose cumulative costs while maintaining plausible deniability (Zheng, 2025). This approach allows the PRC to remain persistently engaged, probing Taiwan's resilience and testing U.S. and allied resolve without committing to overt escalation.

Although U.S. doctrine increasingly acknowledges gray zone competition, responses remain inconsistent and fragmented. Institutional stovepipes continue to separate cyber operations, information operations, economic tools, and military planning, limiting commanders' ability to synchronize effects across domains. Legal and policy constraints further complicate coordination, often slowing decision-making at precisely the moment when speed and coherence are most critical (Braw, 2022). These frictions create exploitable seams that the PRC can leverage to advance its objectives incrementally.

Compounding this challenge are persistent interoperability and integration gaps within combined and joint command and control structures. Effective deterrence in a multidomain environment requires rapid information sharing, aligned decision authority, and synchronized action among allies and partners (Braw, 2022). Yet current command architectures often struggle to integrate partners at the speed required to counter gray zone escalation. When adversary shaping actions occur faster than coalition coordination, deterrence credibility erodes.

The Taiwan scenario magnifies these weaknesses because it is not solely a regional military problem. A crisis in the Taiwan Strait would have immediate global implications, affecting maritime trade, supply chains, alliance credibility, and international norms (Schneider Rasador and Moreira Cunha, 2025). In such an environment, deterrence that relies primarily on the promise of eventual military response risks arriving too late to prevent strategic loss. The PRC may succeed by shaping conditions so that escalation appears inevitable or too costly to resist.

The problem, therefore, is not the absence of military capability, but the absence of a coherent framework to compete effectively before overt conflict (Lundberg, Hacks, and Anderson, 2024). If deterrence is activated only when missiles launch or amphibious forces move, the PRC may already have secured decisive advantage through non-kinetic means. Preventing conflict over Taiwan requires a deterrence posture that operates earlier, integrates multiple domains, and imposes credible costs during the shaping phase rather than after escalation has begun (Zheng, 2025).

3. Purpose

The purpose of this paper is to propose a multidomain deterrence framework capable of preventing a People's Republic of China (PRC) invasion of Taiwan by competing effectively in the gray zone prior to open conflict. Rather than treating deterrence as a function that activates only at the threshold of kinetic war, this paper seeks to reframe deterrence as a continuous, preemptive effort that shapes adversary decision-making across military and non-military domains.

Specifically, the paper advances the concept of an "Inverse Unrestricted Warfare" framework that mirrors and counters the PRC's own strategic approach. By applying the logic of Unrestricted Warfare against the PRC, the framework integrates distributed military denial, non-kinetic cost imposition, cognitive and informational maneuver, and asymmetric disruption into a coherent deterrence strategy aligned with *Force Design*.

The paper's intent is not to present a detailed operational plan for Taiwan defense, but to provide a conceptual and strategic framework that informs *Force Design*, posture decisions, and campaign planning before crisis forces irreversible choices. The framework is designed to help commanders, planners, and policymakers understand how deterrence can be strengthened before escalation by denying the PRC low-cost coercive options, compressing coalition decision timelines, and reinforcing Taiwanese resilience.

Ultimately, the purpose of this study is to demonstrate that deterrence failure is not inevitable if competition remains confined to kinetic considerations (Zheng, 2025). By shaping the shaping fight through parallel, multidomain action, the United States and its allies can impose credible costs, preserve legitimacy, and prevent the PRC from achieving strategic objectives through ambiguity, timing, and coercion.

4. Analysis and Background: Unrestricted Warfare, Gray Zone Competition, and the Need for an Inverse Approach

The strategic context surrounding Taiwan deterrence is best understood through the lens of Unrestricted Warfare, which reconceptualizes conflict as a contest unconstrained by traditional military boundaries. Rather than privileging decisive battlefield engagements, this approach integrates political pressure, economic leverage, cyber operations, legal manipulation, and information campaigns to achieve strategic objectives without triggering conventional escalation. The People's Republic of China (PRC) has adopted this logic as a central feature of its competition strategy, enabling persistent pressure while preserving ambiguity (Qiao & Wang, 1999).

Gray zone competition is the operational manifestation of Unrestricted Warfare. It operates in the space between war and peace, where actions are coercive yet fall short of armed attack (Zheng, 2025). In the Taiwan context, gray zone activities allow the PRC to degrade resilience, influence decision-making, and test alliance credibility without providing a clear casus belli. These actions include cyber intrusions targeting infrastructure and governance systems, economic coercion designed to influence political outcomes, and coordinated disinformation campaigns aimed at eroding public trust (Qiao & Wang, 1999).

A defining characteristic of gray zone competition is its cumulative effect on decision-making conditions. Individual actions may appear manageable in isolation, but collectively they shape conditions that constrain adversary options and increase the likelihood of favorable outcomes without overt conflict (Braw, 2022). This approach exploits the tendency of democratic systems to seek consensus and legal clarity before responding, creating decision latency that can be strategically decisive (Pascoli, Grzegorzewski, 2021).

Traditional deterrence models, which emphasize military denial and punishment after escalation, are poorly suited to this environment. They assume clear thresholds, visible aggression, and linear escalation pathways. In practice, gray zone competition blurs thresholds and exploits ambiguity, allowing the PRC to advance objectives incrementally while avoiding decisive response. As a result, deterrence that relies solely on kinetic superiority risks becoming reactive and ineffective (Zheng, 2025).

The *Force Design* initiative provides a partial answer to this challenge by emphasizing distributed operations, expeditionary resilience, and integration across domains. However, without a broader strategic framework, these capabilities risk being applied narrowly within the military domain (Lundberg, Hacks, and Andersson, 2024). To counter Unrestricted Warfare effectively, distributed denial must be integrated with non-kinetic instruments of power and applied proactively during the shaping phase of competition.

This requirement leads to the concept of an Inverse Unrestricted Warfare approach. Rather than rejecting the logic of Unrestricted Warfare, this approach mirrors it—using parallel, multidomain actions to deny advantage, impose costs, and delegitimize coercion before conflict begins. By competing across the same domains the PRC seeks to exploit, the United States and its allies can disrupt gray zone campaigns, reduce ambiguity, and restore deterrence credibility (Zheng, 2025).

5. The Inverse Unrestricted Warfare Framework

This paper proposes an Inverse Unrestricted Warfare framework as a multidomain deterrence strategy designed to counter the People's Republic of China's (PRC) approach to gray zone competition. Rather than waiting for

escalation into open conflict, the framework seeks to shape the strategic environment in advance by denying coercive advantage, imposing costs, and reinforcing legitimacy across military and non-military domains. The framework is organized into five mutually reinforcing lines of effort that together form a layered deterrence posture.

The central premise of the framework is that deterrence must operate continuously and in parallel across domains, rather than activating sequentially after escalation thresholds are crossed. Military denial alone is insufficient if political resolve, economic stability, and public trust are undermined before kinetic conflict begins (Braw, 2022). Conversely, non-kinetic measures without credible military denial lack coercive weight. The five lines of effort (LOEs) are therefore designed to function as an integrated system rather than as independent activities.

5.1 Line of Effort 1: Military Denial Through Distributed Operations

The first line of effort focuses on denying the PRC the ability to achieve a rapid fait accompli against Taiwan. Distributed operations, as emphasized in *Force Design*, complicate adversary targeting, reduce vulnerability to decapitation, and increase the cost and uncertainty of invasion. By dispersing forces, sensors, and fires across the littoral environment, the Marine Corps contributes to a denial posture that remains resilient under conditions of contested communications and precision strike.

Military denial in this context must assume degraded command and control. Mission command, delegated authorities, and pre-planned actions are essential to maintaining effectiveness when connectivity is disrupted (Lundberg, Hacks, and Anderson, 2024). A denial posture that depends on uninterrupted networks is vulnerable to the very cyber and electronic warfare tactics the PRC is likely to employ during the shaping phase of conflict.

5.2 Line of Effort 2: Non-Kinetic Domain Deterrence

The second line of effort extends deterrence into non-kinetic domains, including cyberspace, economic pressure, and international legitimacy. Gray zone coercion relies on the assumption that these tools can be applied at low cost and with limited risk. Non-kinetic deterrence seeks to deny that advantage by increasing resilience, improving attribution, and pre-positioning credible consequences.

Cyber resilience is central to this effort. If cyberattacks fail to disrupt governance, command and control, or public confidence, their strategic value diminishes. Economic deterrence requires advance coordination with allies to ensure that coercive actions trigger immediate and collective costs rather than delayed, fragmented responses (Pascoli and Grzegorzewski, 2021). Legal and diplomatic measures further reinforce deterrence by exposing coercion and undermining adversary narratives.

5.3 Line of Effort 3: Cognitive and Informational Maneuver

The third line of effort recognizes the cognitive domain as a primary battleground in gray zone competition (Qiao & Wang, 1999). Influence operations, disinformation, and narrative manipulation are designed to erode public trust, weaken resolve, and create a perception of inevitability. Deterrence therefore requires defending public confidence and maintaining narrative coherence during periods of ambiguity and pressure (Braw, 2022).

Operations in the Information Environment provide the means to protect decision-making, reinforce legitimacy, and align coalition messaging. Secure and resilient communications are essential to preventing information vacuums that adversaries can exploit. By treating public trust as operational terrain, this line of effort seeks to deny the PRC the ability to achieve strategic effect through perception shaping alone.

5.4 Line of Effort 4: Asymmetric Disruption and Escalation Options

The fourth line of effort introduces asymmetric disruption options that impose disproportionate costs and uncertainty on the PRC. These options include mobile fires, undersea capabilities, electromagnetic warfare, and other tools that exploit adversary dependencies and vulnerabilities. The objective is not escalation for its own sake, but the creation of credible uncertainty that complicates planning and raises the perceived risk of aggression.

Asymmetric disruption also extends beyond the immediate Taiwan operating area. By highlighting the global economic and political consequences of aggression, this line of effort expands the PRC's cost calculus and reduces confidence that conflict can be contained geographically or economically.

5.5 Line of Effort 5: Preemptive and Parallel Shaping

The fifth line of effort integrates the framework through preemptive and parallel shaping. Rather than sequencing actions after escalation, this approach emphasizes early preparation and simultaneous action across domains. Preemptive shaping does not imply offensive escalation, but deliberate readiness that denies adversaries the benefits of timing, ambiguity, and decision asymmetry.

Parallel shaping ensures that denial, resilience, cost imposition, and narrative alignment are available at the outset of crisis. By compressing response timelines and reducing ambiguity, this line of effort shifts initiative away from the PRC and toward the coalition, strengthening deterrence before conflict becomes unavoidable.

6. Recommendations

To operationalize the Inverse Unrestricted Warfare framework, deterrence must be translated from conceptual alignment into concrete actions that can be implemented during peacetime competition and early crisis shaping. The following recommendations align with the five lines of effort and are intended to strengthen deterrence before escalation occurs.

6.1 Strengthen Distributed Denial and Resilience

Distributed denial capabilities should be designed and exercised under conditions of degraded command and control. Marine Corps forces aligned with *Force Design* should routinely train to operate with mission command, delegated authorities, and preplanned responses that assume communications disruption. Cyber resilience must be treated as an operational requirement rather than an enterprise support function, with defensive cyber capabilities integrated into forward-deployed and expeditionary formations. Exercises should incorporate gray zone conditions such as cyber disruption, information attacks, and economic pressure to reflect the most likely pre-invasion environment (Pascoli and Grzegorzewski, 2021).

6.2 Pre-Coordinate Non-Kinetic Cost Imposition

Non-kinetic deterrence requires credible consequences that are prepared in advance rather than improvised during crisis. The United States and its allies should develop pre-approved economic, legal, and diplomatic response packages tied to clearly defined coercive actions. These packages should be designed to activate rapidly, signaling that gray zone escalation will produce immediate and collective costs. Legal and diplomatic mechanisms should be integrated into operational planning to ensure that coercive actions are documented, attributed, and exposed in near real time (Pascoli and Grzegorzewski, 2021).

6.3 Defend the Cognitive Domain as Operational Terrain

Public trust and political resolve must be treated as critical components of deterrence. Operations in the Information Environment should be integrated into deterrence planning, not reserved solely for wartime execution. This includes pre-aligning coalition messaging, reinforcing Taiwanese civil resilience, and ensuring secure crisis communications that can function under disruption. By maintaining narrative coherence and reducing information vacuums, the coalition can deny the People's Republic of China opportunities to shape perceptions through disinformation and psychological pressure (Zheng, 2025).

6.4 Expand Asymmetric Disruption Options

Asymmetric capabilities that impose disproportionate costs should be prioritized to exploit adversary vulnerabilities. Investments in mobile fires, undersea capabilities, electromagnetic warfare, and other low-cost, high-impact tools can significantly complicate invasion planning and increase uncertainty (Schneider Rasador and Moreira Cunha, 2025). These capabilities should be exercised and demonstrated in ways that contribute to deterrence signaling, reinforcing the perception that aggression will generate cascading and difficult-to-control consequences.

6.5 Institutionalize Preemptive and Parallel Shaping

Deterrence must begin before visible escalation. Planning and posture should emphasize parallel shaping across domains, ensuring that denial, resilience, cost imposition, and narrative alignment are all available at the onset of crisis. Preemptive shaping should be understood as preparedness rather than provocation, focused on reducing ambiguity and compressing response timelines. Readiness metrics should reflect integration and speed of activation rather than platform counts or inventory depth alone.

7. Conclusion and Implementation Implications

In conclusion, deterring a People's Republic of China invasion of Taiwan requires more than conventional military superiority. The PRC's approach to competition, rooted in the logic of Unrestricted Warfare, seeks to achieve strategic objectives through gray zone coercion, multidomain shaping, and perception management before overt conflict begins. In such an environment, deterrence fails not only when military denial collapses, but when political resolve weakens, alliances fracture, and decision-making slows under pressure (Braw, 2022).

This paper advanced an Inverse Unrestricted Warfare framework designed to counter this challenge by competing across the same domains the PRC seeks to exploit. By integrating distributed military denial, non-kinetic cost imposition, cognitive and informational maneuver, asymmetric disruption, and preemptive parallel shaping, the framework offers a layered approach to deterrence that operates before escalation and remains resilient under ambiguity.

Aligned with *Force Design*, this approach emphasizes dispersion, resilience, and integration rather than reliance on centralized systems vulnerable to disruption. It reframes deterrence as a continuous process of shaping conditions, denying low-cost coercion, and imposing credible costs early. In doing so, it reduces the PRC's confidence in achieving objectives through timing, ambiguity, or incremental pressure.

Implementation implications and outcomes are interrelated but not entirely dependent on one another. In LOE 1: Military Denial Through Distributed Operations, implementation requires the dispersion of sensors, shooters, and decision-making nodes throughout the operational environment, enabled by mission command and delegated authorities, with projected outcomes including increased uncertainty and force dispersion within the PLA. In LOE 2: Non-Kinetic Domain Deterrence, implementation requires pre-established actions and counteractions in the cyber domain, ensuring aggression is met with immediate and effective deterrence. LOE 3: Cognitive and Informational Maneuver requires the implementation of secure communications, incorporating OIE and Taiwanese resistance to maintain public trust and political resolve. For LOE 4, implementation involves intentionally resourcing low-cost, high-impact technologies across warfighting domains to create uncertainty and exploit vulnerabilities in the PLA kill chain cycle. In LOE 5: Preemptive and Parallel Shaping, implementation includes establishing metrics that emphasize simultaneous offensive and defensive measures, creating a dynamic deterrence environment.

Ultimately, preventing conflict over Taiwan depends on the ability to shape the shaping fight before commanders are forced to make irreversible decisions under crisis conditions. An Inverse Unrestricted Warfare approach provides a means to do so—preserving initiative, reinforcing legitimacy, and making coercion unreliable. By competing effectively in the gray zone, the United States and its allies can strengthen deterrence, safeguard Taiwan's security, and prevent war before it begins.

Ethics Declaration: Ethical clearance was not required for this research.

AI Declaration: Open-source artificial intelligence tools were used solely for proofreading and citation formatting. All analysis, arguments, and conclusions presented in this paper are the original work of the authors or are derived from appropriately cited sources.

Disclaimer: The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government.

References

Braw, E. (2022). Deterring Gray-Zone Aggression. In *American Enterprise Institute Research Papers*. American Enterprise Institute for Public Policy Research.

Lundberg, J., Hacks, S. and Andersson, K. (2024) 'Refinement of a conceptual model of a military C2 system through low-level goal decomposition', in *Companion proceedings of the 17th IFIP WG 8.1 Working Conference on the Practice of Enterprise Modeling Forum (PoEM 2024)* (M4S, FACETE, AEM, Tools and Demos), Stockholm, Sweden.

Office of the Director of National Intelligence (ODNI) (2022) *2022 Annual Threat Assessment of the U.S. Intelligence Community*. Washington, DC: ODNI.

Pascoli, S.W. and Grzegorzewski, M. (2021) 'Technology adoption in unconventional warfare', *The Cyber Defense Review*, 6(3), pp. 61–74. Available at: https://www.jstor.org/stable/48631155

Qiao, L. and Wang, X. (1999) *Unrestricted warfare*. Beijing: PLA Literature and Arts Publishing House.

Sturmberg, J.P. and Gainsford, L. (2024) 'Complex adaptive organisations: How three-dimensional visualisations can help to understand their structures and behaviours', *Journal of Evaluation in Clinical Practice*, 30(3), pp. 497–502. Available at: https://doi.org/10.1111/jep.13958

Schneider Rasador, G., & Moreira Cunha, A. (2025). The new security grey zone: export controls, emerging technologies and US-China technological rivalry. *Pacific Review*, *38*(6), 1020–1048. Available at https://doi.org/10.1080/09512748.2025.2470222

United Nations (1982) *United Nations Convention on the Law of the Sea*. Signed 10 December 1982, entered into force 16 November 1994. New York: United Nations. Available at: https://www.un.org/Depts/los/convention_agreements/convention_overview_convention.htm

U.S. Department of Defense (2021) *Freedom of Navigation Operations in the South China Sea, 2021*. Washington, DC: Department of Defense. Available at: https://www.defense.gov/

U.S. Department of Defense (2022) *Indo-Pacific Strategy Report*. Washington, DC: Department of Defense.

U.S. Marine Corps (1997) *MCDP 1: Warfighting*. Washington, DC: Department of the Navy.

U.S. Marine Corps (2020) *Force Design 2030*. Washington, DC: Headquarters, U.S. Marine Corps. Available at: https://www.marines.mil/Force-Design-2030/

Zheng, M.F. (2025) *Dragon vs. Eagle*. Bright Summit Press.