

Denial: A Doctrine for Contested Environments

A Defense Monograph

Author: Anton Kaska, Borealis-Traders of New England, LLC

Date: 7 September, 2025

Executive Summary

This monograph introduces and defines Denial as a doctrine for contested environments. It argues that the traditional reliance on platform-centric power-carriers at sea, tanks on land, and aircraft in the air-has become increasingly vulnerable to distributed, low-cost, and adaptive threats. In the 21st century battle-space, survivability no longer rests on protecting a few exquisite assets, but on the endurance of distributed networks that can absorb losses, adapt rapidly, and deny adversaries certainty.

The analysis begins with Ukraine, where Russia's reliance on armor and artillery has been undermined by Ukraine's distributed use of drones and its Sky Fortress network of acoustic sensors. These systems, described by General James Hecker of U.S. Air Forces in Europe as 'extremely cost effective, scalable, and adaptable,' reveal the power of distribution. They demonstrate that decentralization, agility, and multiplicity allow defenders to impose exhaustion on superior forces while denying them victory signals.

From this operational foundation, the monograph distills four principles of Denial: decentralization, agility, multiplicity, and the denial of victory signals. Decentralization ensures that no single strike is decisive. Agility ensures adaptation faster than adversaries can counter. Multiplicity turns cheap systems into enduring strategic pressure. Denial of victory signals denies adversaries the feedback they need to measure progress, forcing them into campaigns of attrition rather than conquest.

The maritime domain illustrates the urgency of applying these principles. China's naval buildup, centered on carriers and large surface combatants, mirrors Russia's reliance on armor. Distributed ISR networks-unmanned vessels, persistent sensors, and autonomous craft-can deny China the certainty it seeks at sea. Analyses by RAND and the Center for Naval Analyses highlight the vulnerability of concentrated fleets to distributed surveillance and targeting networks. Denial at sea mirrors denial on land: traditional fleets face erosion rather than guaranteed control in a distributed environment. Asymmetric adversaries such as Iran and North Korea further demonstrate the diffusion of Denial logic. Iran's 2019 drone swarm attack on Saudi oil facilities imposed billions in damage at minimal cost. North Korea's strategy relies on missile salvos intended to overwhelm layered defenses, imposing disproportionate cost on defenders. Both cases show how limited-resource actors can impose uncertainty and exhaustion on stronger adversaries through distribution and persistence.

These modern examples reflect lessons long recognized but often forgotten. Sun Tzu advised, 'Appear at points which the enemy must hasten to defend; march swiftly to places where you are not expected.' Clausewitz emphasized fog and friction, warning against over-reliance on decisive battle. Cold War strategies of dispersal echoed the same logic. Denial re-frames these enduring lessons in the light of modern technologies that allow distribution at scale.

The monograph concludes by defining Denial as doctrine, not as a product or platform. It is a way of fighting that embraces persistence, ambiguity, and resilience. Its implications are profound. Procurement must emphasize distributed systems over exquisite platforms. Training must prepare forces for decentralized decision-making in contested environments. Strategy must shift deterrence from the promise of decisive retaliation to the assurance of endurance. Denial is not optional; it is the doctrine required to prevail in the 21st century.

Table of Contents

Table of Contents

Executive Summary.....	2
Table of Contents.....	4
Chapter 1: Introduction – Why Platforms Fail.....	7
The Legacy of Platform-Centric Power.....	7
The Changing Character of War.....	7
Why Platforms Fail in Contested Environments.....	8
Denial as Response.....	8
Endnotes.....	8
Chapter 2: Ukraine’s Lessons.....	9
The Drone Revolution.....	9
The Sky Fortress System.....	10
Operational Consequences.....	10
Implications for Denial Doctrine.....	11
Endnotes.....	11
Chapter 3: Principles of Denial.....	11
Decentralization.....	11
Agility.....	12
Multiplicity.....	12
Denial of Victory Signals.....	13
Operational Integration.....	13
Implications for Future Doctrine.....	14
Endnotes.....	14
Chapter 4: The Maritime Domain.....	14
China’s Naval Buildup.....	14

<i>Illustrative Case: Carrier in a Sea of Trawlers</i>	15
ISR and Distributed Networks.....	16
Cost Asymmetry.....	16
RAND and CNA Perspectives.....	16
Comparisons to Cold War Naval Strategy.....	17
Operational Lessons.....	17
Implications for US and Allied Forces.....	17
Endnotes.....	18
Chapter 5: Asymmetric Adversaries.....	18
Iran’s Drone Swarms.....	18
North Korea’s Missile Salvos.....	19
Global Diffusion of Denial Logic.....	19
Implications.....	19
Endnotes.....	20
Chapter 6: Forgotten Lessons.....	20
Sun Tzu and Ancient Wisdom.....	20
Clausewitz and the Fog of War.....	20
Cold War Dispersion.....	21
Why Militaries Forget.....	21
Denial as Rediscovery.....	21
Endnotes.....	22
Chapter 7: Denial Defined.....	22
Denial as Doctrine.....	22
Not a Product, Not a Platform.....	22
Implications for Procurement.....	23
<i>“In 2025, Anduril joined the primes at the carrier’s gate.”</i>	23

Implications for Training.....	24
Implications for Strategy.....	24
Closing Definition.....	24
Endnotes.....	25

Air superiority alone no longer guarantees freedom of action.

Chapter 1: Introduction – Why Platforms Fail

For centuries, military power has been measured by platforms. Nations have counted the number of ships in their fleets, the size of their armored divisions, and the capabilities of their aircraft to gauge their strength. Platforms have not only represented combat power—they have embodied national pride, political influence, and deterrent effect. Yet the assumption that larger or more advanced platforms guarantee advantage is no longer valid. In contested environments, platforms fail. Denial doctrine begins with this recognition: that concentration invites destruction, while distribution ensures endurance. Air superiority alone no longer guarantees freedom of action. A thousand cheap drones, each no larger than a deck of playing cards, can disperse across the rear area in minutes, mapping every forward arming and refueling point, resupply park, and command post. That information, relayed instantly to enemy targeting systems, strips away the protection once assumed by mobility or concealment. Denial doctrine exploits this asymmetry: persistence and multiplicity can neutralize even the most advanced platforms.

The Legacy of Platform-Centric Power

The dominance of platforms in military thinking has deep historical roots. In antiquity, triremes projected naval supremacy. In the industrial age, battleships symbolized national might. In the 20th century, aircraft carriers, armored divisions, and strategic bombers became the measure of global power. The Cold War further entrenched this logic, as superpowers built arsenals of nuclear platforms and massive conventional fleets to deter one another.

Platforms offered tangible symbols of strength. They reassured allies, intimidated adversaries, and concentrated combat power. But their very concentration also created vulnerability. The sinking of the battleship **Prince of Wales** in 1941, the loss of carriers at Midway, and my own experience as an anti-armor NCO in Desert Storm, illustrate this truth. I watched columns of Iraq's much-feared Republican Guard - once thought invincible and combat-tested - collapse under distributed fires. It was not the individual TOW, aircraft, or artillery strike that broke them; it was the unrelenting, multi-axis pressure that stripped them of confidence and options, demonstrating the risks of relying on a few large, high-value systems. These lessons were acknowledged at the time but inconsistently translated into doctrine or procurement.

The Changing Character of War

The 21st century battlefield has accelerated the erosion of platform-centric power. Precision-guided munitions, drones, cyber operations, and distributed ISR networks have reshaped the balance. Platforms that once enjoyed near-invulnerability are now

persistently targeted by cheap, numerous, and adaptive systems. The cost-exchange ratio has inverted. What was once a source of deterrence now represents an inviting target.

Ukraine illustrates this shift most clearly. Russian armored formations, symbols of centralized military power, have been systematically degraded by drones and precision fires. Carriers and destroyers in the South China Sea face the same pressures, as distributed sensors and unmanned craft multiply beyond the capacity of centralized fleets to counter. Iran and North Korea have shown how even limited-resource states can exploit distribution to offset superior platforms.

Why Platforms Fail in Contested Environments

Platforms fail in contested environments for three reasons. First, they concentrate value. The loss of a single carrier, destroyer, or armored brigade represents not only tactical defeat but strategic and political shock. Second, they are slow to adapt. Designed over decades, platforms evolve at a pace far slower than distributed threats that can be improvised in months. Third, they provide clear victory signals. An adversary that sinks a carrier or destroys a tank column can claim decisive success, reinforcing momentum and morale.

Distributed systems invert these dynamics. They disperse value across countless nodes. They adapt rapidly, evolving faster than adversary countermeasures. And they deny victory signals, ensuring that no single strike produces strategic reassurance. In a war of exhaustion, distribution corrodes the adversary's will while preserving one's own.

Denial as Response

Denial emerges as the doctrinal response to the failure of platforms. It does not abandon platforms altogether, but it relegates them to roles where their symbolic and concentrated power can be leveraged without becoming decisive vulnerabilities. Denial insists that survivability must be rooted in distribution, not concentration. The doctrine applies equally on land, at sea, in the air, and in cyberspace. It re-frames deterrence from the ability to strike to the ability to endure.

This monograph proceeds to develop Denial doctrine across domains. Ukraine provides the first case study, revealing how drones and distributed detection have eroded Russian firepower. From there, the principles of Denial are distilled, applied to the maritime domain, observed in asymmetric adversaries, and connected to forgotten lessons of strategy. The conclusion defines Denial formally as doctrine and offers implications for procurement, training, and strategy in the 21st century.

Endnotes

- [1] John Keegan, **The Price of Admiralty: The Evolution of Naval Warfare**, 1988.
- [2] Williamson Murray and Allan Millett, **Military Innovation in the Interwar Period**, 1996.
- [3] "The Future of Warfare in 2030: Project Overview and Conclusions" (2020) .
- [4] "Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience" (2025)

- [5] David E. Johnson, *Learning Large Lessons: The Iraq War* (RAND Corporation, 2007).
[6] Deptula, David A., *Desert Storm at 30: Aerospace Power and the U.S. Military*, War on the Rocks, March 1, 2021

“The assumptions of platform-centric warfare no longer hold.”

Chapter 2: Ukraine’s Lessons

The war in Ukraine has revealed with brutal clarity that the assumptions of platform-centric warfare no longer hold. When Russia launched its full-scale invasion in 2022, it expected massed armor, artillery, and centralized firepower to deliver decisive results. Instead, Russia encountered a Ukrainian defense that adapted with speed and resilience, leveraging distribution, improvisation, and low-cost technologies to impose deliberate denial of enemy victory signals.

The Drone Revolution

From the earliest days of the conflict, small, inexpensive drones became a decisive force multiplier. Ukraine employed commercial quad-copters, fixed-wing unmanned aerial vehicles, and later domestically produced longer-range drones to contest Russia’s reliance on armor and artillery. The effectiveness of these systems lies in their asymmetry. A single drone costing as little as one thousand dollars was capable of disabling or destroying a Russian tank valued in the millions. This inversion of cost and effect revealed the fragility of massed platforms in the face of distributed, expendable threats.

Ukrainian units integrated drones into artillery spotting, intelligence collection, and direct attack roles. Russian convoys that expected to maneuver



Figure 1: photo: armyinform.com.ua

uncontested instead faced constant harassment from above. Drone operators adjusted rapidly, sharing lessons across units and adapting commercial platforms for military use. Even when Russia attempted to jam or intercept drones, Ukraine responded with new tactics, alternate frequencies, and sheer volume. The Russian approach of concentrating resources around large platforms could not adapt at the speed of Ukraine's distributed drone operations.

This dynamic was not limited to front-line combat. Drones gave Ukrainian forces the ability to extend their reach deep into Russian logistics and command nodes. Ammunition depots, supply convoys, and even air bases were struck. The constant pressure from these distributed systems imposed costs far beyond their monetary value. For Denial doctrine, the lesson is simple: distribution can transform inexpensive systems into strategic capabilities.

The Sky Fortress System

Perhaps the most striking Ukrainian innovation is the so-called 'Sky Fortress' network of acoustic detection systems. Built from thousands of sensors, many using the microphones of ordinary cell phones mounted on poles, the system is designed to detect and triangulate the sound of inbound drones. The network is low-cost, resilient, and distributed across Ukrainian cities and rural areas. It provides early warning, enabling defenders to respond before drones reach their targets.

As General James Hecker, Commander of US Air Forces in Europe, stated in 2024: 'These distributed systems are extremely cost effective, scalable, and adaptable in ways that legacy air defense never was.' The Sky Fortress system represents Denial doctrine in practice. Even when individual nodes are destroyed or disabled, the network as a whole persists. No single strike can collapse the system. The system demonstrates that survivability is no longer a function of protecting the largest platform, but of ensuring the endurance of the network.

Operationally, Sky Fortress has reshaped Ukraine's air defense posture. While Ukraine lacks the resources to intercept every drone or missile, its distributed network ensures detection, warning, and adaptability. Even when strikes succeed, Russia cannot claim certainty of success. Civilian infrastructure is defended not by an impenetrable shield, but by a flexible

and persistent net of distributed sensors. For Denial doctrine, Sky Fortress demonstrates the principle of multiplicity-small, cheap, and expendable nodes combining into a resilient whole.

Operational Consequences

The Ukrainian experience highlights the weakness of centralized doctrine in the face of distributed opposition. Russia sought to apply overwhelming firepower in decisive blows, expecting Ukrainian defenses to collapse under the weight of attrition. Instead, Ukraine absorbed strikes, adapted, and imposed continuous costs. Every Russian advance was met with distributed resistance, from drones to improvised fires. The result was not decisive victory, but exhaustion.

For NATO and allied militaries, the implications are profound. Denial cannot be treated as a secondary tactic. It must be recognized as doctrine. The survivability of future forces will depend not on the protection of a few exquisite assets, but on the endurance of networks composed of many cheap, expendable, and adaptable systems. This requires a shift in procurement, training, and strategic planning. The Ukrainian case proves that adversaries relying on centralized platforms will bleed resources against distributed denial.

Implications for Denial Doctrine

Ukraine validates the principles of Denial at the operational level. Decentralization ensured that the destruction of individual drones or sensors did not collapse defenses. Agility allowed Ukrainian forces to adapt faster than Russia could counter. Multiplicity meant that no single victory could reassure Russia of progress. And most importantly, the denial of victory signals undermined Russia's ability to measure success. When no strike confirmed victory, Russia was forced into a war of exhaustion rather than conquest.

For the future, Denial doctrine must be understood as more than an emergency improvisation. It is a blueprint for operating in contested environments. Whether on land, at sea, or in the air, distribution transforms vulnerability into resilience. Ukraine has proven that even against a numerically superior adversary, distributed systems can impose strategic ambiguity and shift the balance of power.

Endnotes

[1] How Ukraine turned mobile phone microphones into an air defense network, FlightGlobal, 2024.

[2] US General James Hecker, quoted in The War Zone, 2024, on Ukraine's acoustic detection systems.

[3] Reports on Ukrainian drone warfare, BBC, 2023.

[4] CSIS, "Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience," 2025.

Chapter 3: Principles of Denial

Doctrine cannot rest on anecdotes or isolated examples. To be useful, it must be distilled into principles that can guide planning, procurement, and operations across multiple domains. Denial, as revealed in the fighting in Ukraine and demonstrated in other theaters, rests on four interlocking principles: decentralization, agility, multiplicity, and the denial of victory signals. Each principle has been proven in combat, and each offers lessons for future contested environments. In this chapter I expand on each principle in turn, grounding them in operational evidence from Ukraine, the South China Sea, Iran, and North Korea.

Decentralization

Decentralization is the foundation of Denial. In a decentralized system, no single node is critical to the function of the whole. If one element is destroyed, others persist and adapt. Ukraine's Sky Fortress network of acoustic sensors offers the clearest operational proof of this principle. Built from thousands of distributed microphones, often repurposed from ordinary cell phones, the system detects incoming drones across a vast territory. No single strike can eliminate the network. Even if dozens of nodes are lost, the system continues to function.

Russia's centralized doctrine, by contrast, relied heavily on command posts and concentrated artillery positions. When Ukrainian drones or HIMARS strikes targeted these concentrations, entire sectors of Russian defense collapsed. This asymmetry highlights the strength of decentralization. Denial doctrine demands that critical functions be spread across networks rather than concentrated in vulnerable nodes.

Maritime operations demonstrate the same lesson. China's carriers and large surface combatants are potent symbols, but they represent centralized vulnerability. A fleet dependent on a handful of large platforms can be blinded or paralyzed by the loss of a few key assets. Distributed ISR networks-composed of unmanned surface vessels, persistent sensors, and smaller manned craft-reflect the opposite approach. They survive not by invincibility, but by dispersal. Denial doctrine seeks survivability through decentralization, ensuring that no strike can be decisive.

Agility

Agility is the ability to adapt faster than platforms can maneuver or adversary systems can evolve. Ukraine's drone operators demonstrated agility in practice. When Russia attempted to jam communications, Ukrainian units shifted frequencies, altered tactics, and increased redundancy. Operators experimented daily, modifying commercial drones with new payloads, navigation systems, and software. This bottom-up innovation cycle outpaced Russia's centralized adaptation processes.

Agility also appears in Iran's drone warfare. Constrained by sanctions, Iran developed a diverse portfolio of UAVs that can be rapidly reconfigured for different missions. These drones have been exported and adapted by proxies, who modify them further for local

conditions. This demonstrates the agility of distributed systems compared to the slow modernization cycles of conventional forces.

In maritime contexts, agility manifests in the use of autonomous ISR craft. Small unmanned vessels can change patrol patterns daily, confusing adversary attempts to map their routes. A destroyer's movements can be tracked, but a swarm of low-cost ISR craft can be agile, unpredictable, and persistent. Denial doctrine requires this constant adaptation, ensuring that distributed forces never present a stable target.

Multiplicity

Multiplicity is the multiplication of small units into a force that overwhelms by scale. In Ukraine, the sheer volume of drones imposed constant pressure on Russian forces. Even when individual drones were intercepted, more were launched. The cost asymmetry was staggering: Russia expended expensive interceptors against drones costing a fraction of the price. The psychological toll of constant drone harassment was as significant as the physical damage.

North Korea's missile strategy reflects the same principle. Lacking the resources to compete with advanced missile defenses, North Korea has pursued the logic of salvos-launching dozens of missiles simultaneously to overwhelm interception systems. Even if many are destroyed, some will penetrate. The cost burden of interception rests disproportionately on the defender. This is multiplicity in practice: survivability through scale, not through the strength of any single system.

At sea, multiplicity translates into swarms of unmanned vessels and sensors. China's large warships cannot be everywhere at once. Swarms of unmanned systems, spread like a net stretched too wide to escape, can impose surveillance and harassment beyond the reach of centralized fleets. Denial doctrine embraces multiplicity as a strategic principle: the conversion of cheap, numerous systems into enduring force.

Denial of Victory Signals

The most novel principle of Denial is the deliberate denial of enemy victory signals. In traditional warfare, battles and campaigns were measured by visible outcomes: territory gained, enemy forces destroyed, platforms sunk. In a distributed environment, these measures lose coherence. Russia has destroyed thousands of Ukrainian drones, yet this destruction has not produced strategic reassurance. Every loss is replaced. Every strike leaves ambiguity.

This uncertainty corrodes adversary decision-making. Without reliable signals of progress, Russia has been forced into a war of exhaustion. In the maritime domain, distributed ISR networks impose the same effect. A Chinese fleet that destroys dozens of small surveillance craft cannot be confident it has cleared the battle-space. Surveillance persists. Uncertainty endures. This is the essence of Denial: victory signals withheld, leaving adversaries uncertain whether their actions achieve anything of value.

Iran's drone operations further illustrate this principle. Saudi oil facilities struck by swarms of Iranian drones could not be definitively secured even after defensive upgrades. Each subsequent strike or attempted strike left uncertainty about the integrity of defenses. Denial doctrine weaponizes ambiguity, ensuring adversaries are denied the clarity needed to sustain campaigns.

Operational Integration

These four principles—decentralization, agility, multiplicity, and denial of victory signals—do not operate in isolation. In Ukraine, distributed systems combined to turn drones and acoustic sensors into a coherent defensive posture. In the South China Sea, the same logic could apply at sea, where unmanned vessels and sensors are beginning to emerge as a persistent maritime presence.

Denial is most effective when its principles reinforce each other. Decentralization disperses value, which enables agility by giving units freedom to adapt without risking the whole. Agility sustains multiplicity, as rapid adaptation keeps numerous systems relevant against evolving threats. Multiplicity deepens the denial of victory signals, because no single strike can assure success against such scale. And the denial of victory signals in turn strengthens decentralization, eroding adversary confidence in targeting and control. Together, these dynamics form a doctrine suited for contested environments where certainty is rare and exhaustion is decisive.

Implications for Future Doctrine

For NATO, the United States, and allied militaries, the implications are urgent. Procurement must prioritize distributed systems over exquisite platforms. Training must prepare forces to operate in decentralized networks rather than centralized hierarchies. Strategic planning must embrace denial as doctrine, ensuring that future conflicts do not rely on fragile concentrations of power. Adversaries are already adapting. Denial must be institutionalized if the West is to prevail in contested environments.

Endnotes

[1] How Ukraine turned mobile phone microphones into an air defense network, FlightGlobal, 2024.

[2] U.S. General James Hecker, quoted in The War Zone, 2024, on Ukraine's acoustic detection systems.

[3] CRS, China Naval Modernization: Implications for U.S. Navy Capabilities, 2024 (updated).

[4] BBC, 'Iran Drone Attack on Saudi Oil Facilities,' 2019.

[5] Missile Defense Project, "North Korea Launches No-Dong Missile Salvo," 2016. .

Chapter 4: The Maritime Domain

The sea has always been a proving ground for doctrine. Control of the maritime domain has shaped the fate of nations, from the triremes of antiquity to the carrier strike groups of today. Yet the assumptions that once underpinned naval supremacy are eroding. Denial

doctrine, proven on land in Ukraine, is no less relevant at sea. In fact, the maritime domain magnifies the vulnerabilities of centralized, platform-centric power. Fleets concentrated around a few high-value assets face the same pressures as tank columns under drone assault. Distribution, persistence, and the denial of victory signals now determine survivability at sea as much as they do on land.

China's Naval Buildup

China's naval modernization has been rapid and ambitious. The People's Liberation Army Navy (PLAN) now fields multiple aircraft carriers, advanced destroyers, and a steadily expanding submarine fleet. These platforms are designed to project power, intimidate neighbors, and contest US and allied presence in the South China Sea. Yet for all their potency, they represent centralized vulnerability. Each carrier or large surface combatant is a node whose destruction would reverberate across China's maritime posture.

This reliance on concentrated fleets mirrors Russia's reliance on armor in Ukraine. Large, expensive, and symbolically powerful, they dominate planning and doctrine. But like tanks under constant drone assault, they are increasingly exposed to distributed, low-cost, and persistent threats. Denial doctrine forces us to recognize that naval power cannot rest on a few exquisite platforms when adversaries can impose uncertainty with many cheap ones.

Illustrative Case: Carrier in a Sea of Trawlers

Carrier strike groups are designed to project power in blue water, where the battle-space is clean and ranges are long. Yet in coastal or semi-enclosed seas, carriers inevitably encounter dense civilian traffic – fishing fleets, merchant convoys, or local ferries. These contacts are lawful, expected, and often unavoidable. Avoidance is not always an option when geography or mission requires presence in congested waters.



Figure 2: photo: US Navy

escorts must adjust posture. None of this necessarily escalates into combat, but each ambiguous contact consumes limited bandwidth and erodes efficiency.

In such an environment, ambiguity becomes the adversary's ally. Each small vessel may be nothing more than a fishing boat. But when dozens appear at once, track parallel to the group, or maneuver unpredictably near the formation, the strike group must allocate attention. Aircraft are tasked to identify, helicopters are launched to overfly, and

Denial in this context is not about sinking ships. It is about constraining freedom of action – forcing a superior fleet to treat every anomaly as a potential threat. The result is a battle-space where vigilance itself becomes a resource under pressure. For doctrine, the lesson is clear: multiplicity and ambiguity, even when individually innocuous, can generate friction that complicates operations for the most capable forces afloat.

The People's Liberation Army Navy mirrors the broader PLA: impressive modernization, rapid growth, and increasing sophistication, but limited skill in sustained deployments. PLAN shipyards are producing carriers and destroyers at speed, yet the fleet remains largely a regional force with weak logistics and uneven proficiency at extended operations. Reports from overseas rotations show clumsy coordination and short legs, underscoring that numbers alone do not equal global reach. Still, in its own backyard – the first island chain and South China Sea – the PLAN's mass and proximity combine with land-based systems to create a formidable denial environment.

ISR and Distributed Networks

Intelligence, surveillance, and reconnaissance (ISR) is the nervous system of maritime operations. Without it, fleets cannot maneuver effectively, target adversaries, or maintain situational awareness. Traditionally, ISR has relied on large assets: maritime patrol aircraft, satellites, and sophisticated warships with powerful sensors. Denial challenges this model by distributing ISR across countless smaller nodes.

Unmanned surface vessels, underwater gliders, airborne drones, and fixed maritime sensors form networks that persist even when individual elements are destroyed. A

destroyer may sink, but the loss of a single unmanned vessel has no strategic consequence. Surveillance continues, uncertainty endures. This is decentralization applied to ISR. As RAND has noted, 'distributed maritime networks can impose disproportionate costs on concentrated fleets by denying them the assurance of stealth or surprise.'

The US Navy has begun experimenting with these approaches, from unmanned surface vessels operating in swarms to persistent undersea sensors. Allies, too, are adapting, with Japan and Australia investing in distributed ISR assets. But China's concentration on carriers and destroyers suggests it has not yet internalized the vulnerability of centralized ISR.

Cost Asymmetry

The cost asymmetry of distributed maritime denial mirrors the cost asymmetry of drones on land. A billion-dollar destroyer can be tracked, harassed, or neutralized by dozens of small unmanned ISR craft costing a fraction of the price. Each cheap vessel imposes a defensive burden out of proportion to its value. For China, this means that each carrier strike group faces an ocean of uncertainty. For the United States and allies, it means investment in distributed ISR multiplies the cost to adversaries without equivalent expense.

Iran demonstrated this logic in 2019 when swarms of drones attacked Saudi oil facilities. Though the context was land-based, the principle carries to sea: small, cheap attackers imposed billions in damage. North Korea's missile salvos reveal a similar logic, forcing defenses to expend expensive interceptors against numerous cheap targets. In the maritime domain, ISR craft and sensors replicate this asymmetry by imposing persistent surveillance and attrition against high-value platforms.

RAND and CNA Perspectives

RAND Corporation and the Center for Naval Analyses (CNA) have both highlighted the vulnerability of concentrated fleets in the South China Sea. RAND's 2023 study on Chinese naval modernization warned that 'large surface combatants face disproportionate risk in contested littorals when distributed ISR networks can provide targeting data to numerous small platforms.' CNA has emphasized the value of unmanned ISR swarms in complicating adversary planning, noting that 'the denial of certainty at sea is as powerful as the denial of maneuver on land.' These analyses reinforce the operational case for Denial doctrine in the maritime domain.

Comparisons to Cold War Naval Strategy

During the Cold War, US naval strategy emphasized forward presence and concentration of power. Carrier strike groups were the centerpiece of deterrence. This posture relied on the assumption that concentrated power could deter aggression through visible, decisive superiority. Denial challenges this assumption. In contested environments, concentrated power invites distributed challenge.

Cold War dispersal doctrines did exist, particularly in NATO's plans for surviving a Warsaw Pact strike. Yet these were secondary to the dominant emphasis on large platforms. Today,

Denial reasserts dispersal as doctrine, not contingency. Distribution is no longer a fallback plan but the primary means of survival in contested seas.

As those of us who served in Europe often joked, the Berlin Brigade – and much of NATO’s forward presence – was less a shield than a speed-bump. The real plan relied on holding long enough for reinforcements from across the Atlantic to reach prepositioned stocks. It was deterrence through visibility rather than survivability, a posture that Denial doctrine deliberately overturns.

Today, Denial reasserts dispersal as doctrine, not contingency. Distribution is no longer a fallback plan but the primary means of survival in contested seas.

Operational Lessons

Distributed ISR networks deny adversaries the certainty they need to maneuver effectively. China may destroy dozens of small surveillance craft, yet still find itself under observation. Every strike leaves ambiguity. This mirrors Russia’s experience in Ukraine: thousands of destroyed drones did not translate into strategic progress. In both cases, the denial of victory signals corrodes adversary planning.

For the United States and allies, the operational lesson is clear. Investment in distributed ISR must accelerate. Exercises must focus on integrating unmanned systems into fleet operations. Doctrine must assume that high-value platforms will be targeted and may be lost, and that survivability will rest on distributed networks that endure even under attrition. Denial is not theoretical-it is operationally validated and strategically necessary.

Implications for US and Allied Forces

For US and allied forces, adopting Denial in the maritime domain requires shifts in procurement, doctrine, and training. Procurement must prioritize unmanned ISR, persistent sensors, and distributed networks. Doctrine must shift from platform-centric deterrence to denial-based endurance. Training must prepare sailors to operate in decentralized environments where decision-making is distributed and survivability rests on persistence rather than invulnerability.

China’s naval buildup cannot be matched ship for ship without prohibitive cost. Denial offers a different path: imposing uncertainty through distribution, exhausting adversaries, and ensuring that every strike feels wasted. This is the future of maritime operations in contested seas. Denial doctrine must be embraced if the West is to maintain strategic advantage.

Endnotes

[1] Naval Logistics in Contested Environments: Examination of Stockpiles and Industrial Base Issues”, 2024.

[2] RAND Corporation, Understanding and Countering China’s Maritime Gray Zone Operations, 2024.

[3] CNA, Russia's Use of Uncrewed Systems in Ukraine, 2023

[4] BBC, 'Iran Drone Attack on Saudi Oil Facilities,' 2019.

[5] CSIS, "The Burgeoning North Korea Missile Threat," 2022

Chapter 5: Asymmetric Adversaries

Denial is not only relevant to great power competition. It is increasingly evident in the strategies of asymmetric adversaries such as Iran and North Korea. These states lack the resources to compete symmetrically with the United States, NATO, or regional powers, yet they have found in distribution and persistence, a means of imposing costs and uncertainty. This chapter examines how Iran and North Korea apply principles of Denial through drones, missiles, and unmanned systems, and the implications for global contested environments.

Iran's Drone Swarms

Iran has become a pioneer in the operational use of distributed unmanned aerial vehicles. The attack on Saudi oil facilities in September 2019 revealed the scale and effectiveness of this approach. Swarms of drones and cruise missiles penetrated defenses and caused billions of dollars in damage to key infrastructure. The cost to Iran was minimal compared to the impact. This asymmetry is the essence of Denial: imposing exhaustion and uncertainty through cheap, numerous, and persistent systems.

Since then, Iran has exported UAVs to proxies across the Middle East, including Hezbollah and the Houthis. These groups have used drones for reconnaissance and attacks on shipping, further extending Iran's distributed networks. The proliferation of these systems demonstrates that Denial is not limited to state militaries but can be adopted by non-state actors with access to low-cost technology.

Iran's strategy is to stretch adversaries thin, forcing them to defend against constant harassment. Each drone may be individually cheap and expendable, but in aggregate they impose unsustainable costs on air defenses and patrol forces. As one Western analyst observed, 'Iran has redefined air power for the budget-constrained state, showing that persistence and scale can outweigh sophistication.'

North Korea's Missile Salvos

North Korea applies Denial principles through its missile forces. Lacking the ability to field large numbers of advanced precision weapons, Pyongyang relies on salvos to overwhelm defenses. Dozens of missiles are launched simultaneously, saturating interception systems. Even if most are destroyed, some inevitably penetrate. This strategy imposes uncertainty on defenders, who cannot be sure of their ability to stop every strike.

This approach reflects multiplicity in its purest form. Quantity becomes a form of quality when defenses are saturated. The cost burden falls on defenders, who expend expensive interceptors against cheap offensive weapons. The United States, South Korea, and Japan are forced to invest in missile defenses that may never provide full reassurance. Denial doctrine explains why North Korea continues to prioritize missile development despite

economic hardship: it provides a way to impose exhaustion and uncertainty on stronger adversaries.

North Korea has also experimented with unmanned aerial vehicles and underwater drones, further extending its distributed arsenal. Though often rudimentary, these systems reinforce the principle that survivability is found in persistence and dispersion, not sophistication alone.

Global Diffusion of Denial Logic

Iran and North Korea illustrate the global spread of Denial logic. Other states are observing and adapting. Russia has employed Iranian-made Shahed drones against Ukraine. China has studied Iranian swarm tactics and North Korean salvo strategies. Non-state actors from Yemen to Ukraine have improvised their own distributed systems. The barriers to entry are low, and the appeal is high. Distribution offers a way to challenge superior powers without matching their expenditures.

For the United States and its allies, this means that Denial is not a doctrine limited to peer competition. It is the future of asymmetric conflict globally. From oil infrastructure in the Gulf to shipping lanes in the Red Sea, distributed threats are becoming the norm. Denial doctrine provides the framework to understand and counter these strategies, but it also warns us that adversaries are embracing them faster than many Western institutions.

Implications

Iran and North Korea show that Denial can be pursued with limited resources. This has several implications. First, traditional measures of military power-GDP, defense spending, or platform inventories-underestimate the ability of small states to impose strategic costs. Second, missile defenses and air defenses cannot be relied upon alone; distributed threats must be met with distributed defenses. Third, the psychological impact of Denial-constant uncertainty, denial of victory signals-can destabilize deterrence calculations even when physical damage is limited.

For Western planners, the challenge is twofold: to prepare to counter Denial tactics while also learning from them. The diffusion of Denial logic means that doctrine must adapt not only to peer adversaries like Russia and China but also to regional challengers and non-state actors who wield distribution as a weapon of the weak. Ignoring these lessons risks repeating the same surprise that Russia faced in Ukraine.

Endnotes

[1] BBC, 'Iran Drone Attack on Saudi Oil Facilities,' September 2019.

[2] CSIS Missile Defense Project, "Missiles of North Korea" (Missile Threat database page), 2022.

[3] Iran's Military Interventions: Patterns, Drivers, and Signposts" (2021)

[4] CNA, Drones Over Ukraine: Commercial Technologies in Combat, 2023.

Chapter 6: Forgotten Lessons

History rarely offers us new principles of war. More often, it reminds us of truths we have allowed ourselves to forget. Denial doctrine is not an invention of the 21st century. Its elements—distribution, deception, and persistence—can be found in the writings of Sun Tzu, the campaigns of classical antiquity, and the strategies of the Cold War. What is new is not the principles themselves but the technologies that allow them to be applied at unprecedented scale. In this chapter I explore the forgotten lessons of military history that underpin Denial and explain why modern militaries so often fail to remember them until crisis arrives.

Sun Tzu and Ancient Wisdom

Sun Tzu's **The Art of War**, written over two millennia ago, repeatedly emphasizes the importance of deception, dispersion, and uncertainty. He wrote: 'Appear at points which the enemy must hasten to defend; march swiftly to places where you are not expected.' This principle captures the essence of Denial. By distributing forces and exploiting surprise, commanders impose exhaustion rather than offering decisive targets.

Other ancient strategists echoed similar principles. The Roman avoidance of pitched battle during Hannibal's invasion, favoring harassment and attrition, demonstrated an early form of Denial. What matters is not the destruction of the enemy's forces in a single battle but the corrosion of their will and capacity to sustain the campaign. These lessons have been known for centuries, yet they are often discarded in favor of the allure of decisive engagements.

Clausewitz and the Fog of War

Carl von Clausewitz, writing in the 19th century, emphasized the fog and friction of war. He cautioned against over-reliance on decisive battle, noting that uncertainty and chance dominate combat. Denial doctrine aligns with this view. By denying victory signals, distributed forces magnify fog and friction, forcing adversaries into indecision. The inability to measure success creates a campaign defined by exhaustion rather than resolution.

"The U-boats did not seek decision — they sought denial."

Clausewitz also recognized the danger of pursuing absolute war. Denial offers an alternative: not the pursuit of destruction, but the deliberate imposition of ambiguity. This logic is echoed in the Battle of the Atlantic during World War II. German U-boats never sought a decisive clash with Allied fleets; their goal was to deny Britain certainty of supply by imposing persistent attrition and ambiguity at sea. The campaign remains a case study for naval officers today in how distributed, low-cost forces can magnify fog and friction against superior platforms.

Cold War Dispersion

The Cold War provides more recent evidence of the enduring value of distribution. NATO's defense plans emphasized dispersal of aircraft, logistics, and command nodes to survive a Soviet first strike. US submarine forces embodied persistence and denial, ensuring second-

strike capability even if surface fleets were destroyed. These strategies were rooted in the same logic that animates Denial today: survivability through dispersion, endurance through persistence.

Yet even during the Cold War, the allure of large platforms remained dominant. Carrier strike groups, nuclear bombers, and armored divisions were celebrated as symbols of strength, even as planners quietly prepared dispersal strategies. The tension between concentration and distribution persisted. Denial argues that in the 21st century, distribution must become doctrine rather than contingency.

Why Militaries Forget

Why do militaries repeatedly forget the lessons of distribution? Part of the answer lies in politics and psychology. Large platforms are visible symbols of national power. They provide reassurance to domestic audiences and deterrence through presence. A drone swarm or dispersed sensor net does not carry the same symbolic weight as an aircraft carrier. As a result, states invest in platforms that reassure politically even when doctrine would demand distribution.

“Denial favors the nimble over the entrenched.”

Institutional inertia also plays a role. Militaries build careers, industries, and bureaucracies around the procurement and operation of large platforms. Shifting to distributed systems threatens entrenched interests. Finally, there is the allure of decisive victory. Commanders and policymakers alike prefer the clarity of decisive engagements over the ambiguity of drawn-out campaigns. Denial, by contrast, embraces ambiguity as a weapon. By contrast, firms such as Anduril and Palantir have built reputations for agility, marketing distributed and software-centric systems as faster, cheaper, and more adaptable alternatives – a posture more aligned with Denial logic.

Denial as Rediscovery

Denial is less a new invention than a rediscovery of principles long known but often ignored. What makes it powerful today is the convergence of technology and necessity. Cheap drones, unmanned vessels, distributed sensors, and resilient communications make it possible to apply ancient principles at unprecedented scale. What Sun Tzu described in theory, and what Cold War planners prepared for in contingency, is now the foundation of operational reality. Denial re-frames forgotten lessons for the 21st century battlefield.

Endnotes

[1] Sun Tzu, **The Art of War**, various translations.

[2] Carl von Clausewitz, *On War*, 1832.

[3] RAND Corporation, *Air Base Attacks and Defensive Counters*, 2015

[4] RAND Corporation, *Naval Logistics in Contested Environments*, 2024

Chapter 7: Denial Defined

The preceding chapters have examined the operational evidence for Denial across land, sea, and asymmetric conflicts, and connected it to lessons long known but too often forgotten. In this final chapter, I define Denial as a doctrine, distinguish it from other approaches, and outline its implications for procurement, training, and strategy. Denial is not a theory to be debated in abstract-it is a doctrine already in practice, shaping conflicts from Ukraine to the South China Sea.

Denial as Doctrine

Denial is a doctrine for contested environments. It accepts that concentration breeds vulnerability while distribution creates resilience. It rejects the assumption that victory comes from decisive battle or the destruction of enemy forces in a single stroke. Instead, Denial redefines success as endurance, ambiguity, and exhaustion imposed on the adversary. It turns every strike into a question mark, ensuring that campaigns devolve into wars of attrition rather than conquests.

Denial is not passive. It does not mean waiting to absorb blows. It is active resistance through distribution, agility, multiplicity, and the deliberate denial of victory signals. It is a doctrine of persistence that forces adversaries into indecision, eroding their will as much as their material strength.

Not a Product, Not a Platform

Denial must not be mistaken for a single product, technology, or platform. It is not defined by drones, unmanned vessels, or sensors alone. These are embodiment's of its principles, but not its essence. Denial is a way of fighting-a lens through which technologies are applied. The danger of reducing Denial to a procurement program is that it will be captured by the same institutional inertia that favors large platforms.

Instead, Denial must remain a doctrinal concept. Procurement decisions should be tested against its principles: Does this system increase decentralization? Does it enhance agility? Does it scale to provide multiplicity? Does it deny adversaries reliable victory signals? If the answer is no, then the system may be ill-suited for contested environments.

Implications for Procurement

For procurement, Denial demands a shift away from over-investment in a small number of exquisite platforms. This does not mean carriers, destroyers, or advanced aircraft are obsolete. It means their role must be reconsidered within a distributed framework.

Investment must flow toward unmanned systems, resilient communications, and persistent ISR networks. Procurement must emphasize scale and survivability over perfection. Some

services are already beginning to shift in this direction, experimenting with faster, more adaptable systems. A recent Navy program illustrates the point.



Figure 3: photo: created using AI

“In 2025, Anduril joined the primes at the carrier’s gate.”

In September 2025, the U.S. Navy awarded conceptual design contracts for an autonomous, carrier-based combat drone. The list of recipients read like a roll call of industry titans—Boeing, Northrop Grumman, General Atomics, Lockheed Martin—and, unexpectedly, Anduril. For a startup founded less than a decade earlier, being placed alongside the primes was more than symbolic. It signaled that Denial logic—favoring speed, scale, and adaptability over protracted platform cycles—has broken into the highest levels of naval procurement. For the traditional defense giants, the presence of an agile competitor in their lane was a reminder that institutional inertia is no longer unchallenged.

This example is emblematic rather than unique – across all services, experiments with unmanned systems, modular platforms, and distributed networks are already underway. The question is whether procurement culture can sustain the shift beyond pilot projects.

This also implies a need for modularity and adaptability. Systems must be capable of rapid reconfiguration, as Ukraine has shown with drones and Iran with UAV proliferation. The pace of adaptation must outstrip the pace of adversary countermeasures. Procurement cycles measured in decades cannot deliver Denial. Innovation cycles must be measured in months.

Implications for Training

Training must adapt as much as procurement. Denial depends on decentralized decision-making. Operators at the tactical edge must be empowered to adapt and innovate. Training must prepare them to operate in degraded environments where communications may be intermittent and centralized control impossible. Exercises must simulate distributed operations, attrition, and ambiguity. Leaders must be comfortable with uncertainty, recognizing that Denial thrives in the fog of war rather than seeking to eliminate it.

This will require cultural change. Militaries accustomed to rigid hierarchies and centralized control must embrace bottom-up adaptation. Ukraine's experience demonstrates that distributed innovation can outpace centralized adaptation. Denial requires that training reward initiative, experimentation, and resilience rather than conformity.

Implications for Strategy

Strategically, Denial re-frames deterrence. Traditional deterrence rested on the threat of decisive retaliation. Denial rests on the assurance of endurance. It tells adversaries not that we can destroy them in a single stroke, but that they cannot defeat us in one. It promises exhaustion, ambiguity, and the corrosion of will. This form of deterrence is no less powerful-it may in fact be more credible, because it does not depend on the illusion of invulnerability.

Denial also has implications for alliances. Distributed networks are not bound by national borders. NATO, for example, already shares ISR across member states, but deeper integration – pooling unmanned assets, sensors, and data into persistent, distributed networks – would create new layers of resilience. The Indo-Pacific can do the same, moving beyond episodic exercises toward continuous, networked surveillance. This creates strategic depth that no single platform or nation can provide alone.

Closing Definition

Denial is the doctrine of contested environments. It is defined by four principles: decentralization, agility, multiplicity, and the denial of victory signals. It is validated by Ukraine's defense, by the vulnerability of China's fleets, by the persistence of Iran's drones, and by the salvos of North Korea. It is grounded in the forgotten wisdom of Sun Tzu, Clausewitz, and Cold War dispersion. It is not a product to be purchased or a platform to be built. It is a way of war for the 21st century.

The next conflict will not be won by the largest platform or the most expensive weapon. It will be won by the doctrine that turns every strike into ambiguity, every advance into exhaustion, and every claim of victory into doubt. Denial begins with the recognition that concentrated platforms fail – and ends with the assurance that endurance defines survivability. That is Denial.

Endnotes

[1] RAND, “Command and Control in U.S. Naval Competition with China” (2020).

[2] CSIS, “Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience,” 2025

[3] CNA “Russia’s Use of Uncrewed Systems in Ukraine” (2023)