

OCTOBER 2026

The Art of Swarming

*Launched Effects and the Future of
Mass on the Modern Battlefield*

AUTHOR

Benjamin Jensen

A Report of the CSIS Futures Lab

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES



OCTOBER 2026

The Art of Swarming

*Launched Effects and the Future of
Mass on the Modern Battlefield*

AUTHOR

Benjamin Jensen

A Report of the CSIS Futures Lab

© 2026 by the Center for Strategic and International Studies.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Center for Strategic and International Studies (CSIS). CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Cover: Nico Vacca/Generated using Gemini and ChatGPT/CSIS

Contents

Executive Summary	1
Introduction	5
Launched Effects	15
Creating an Operational Framework	24
Swarming Against the Integrated Air Defense	35
<i>Case Study: Kaliningrad</i>	37
Swarming Against Integrated Sea Control	42
<i>Case Study: The South China Sea</i>	49
Swarming Against a Defense in Depth	55
<i>Case Study: NATO's Eastern Flank</i>	57
Recommendations	64
Conclusion	75
About the Author	78
About CSIS	79
Endnotes	80

Acknowledgements

This report is based on insights gleaned from a mix of military support, studies, and wargames that have evolved over years and across continents from work in and outside of government. Like all large projects, that means it stands on the shoulders of others. Specifically, I would like to thank Nico Vacca for his research support and CSIS's publications team. Second, multiple external reviewers contributed thoughtful comments in their personal, non-government capacity, including David Blair, Curtis Wilson, and Jaron Wharton. This project also benefits from earlier ongoing discussions about unmanned systems and warfare, including Scott Cuomo and Michael Horowitz. It also would not be possible without years of wargames and debates with students at Marine Corps University Command and Staff College and the School of Advanced Warfighting.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

Abbreviations

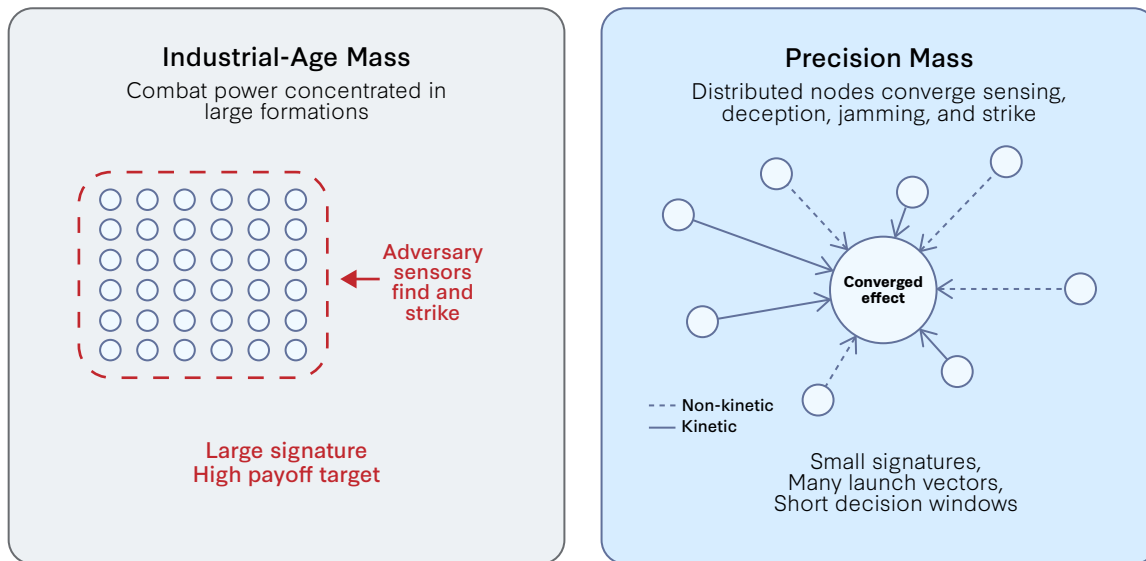
A2/AD	Anti-access/area denial
A2LE	Advanced Air-Launched Effects
AFO	Advanced force operations
AWACS	Airborne warning and control system
BACN	Battlefield airborne communications node
C2	Command and control
C2CM	Command and control countermeasures
C5ISR-T	Command, control, communications, computers, combat systems, intelligence, surveillance, reconnaissance, and targeting
C-UAS	Counter-unmanned aircraft system
DAWG	Defense Autonomous Warfare Group
DRPM-UxS	Direct Reporting Portfolio Manager for Unmanned Systems
ELINT	Electronic intelligence
EM	Electromagnetic
EW	Electronic warfare
FPV	First-person view
GA-ASI	General Atomics Aeronautical Systems, Inc.
IADS	Integrated air defense system
IAMD	Integrated air and missile defense
IP	Intellectual property
ISR	Intelligence, surveillance, and reconnaissance
LE/LEs	Launched effects
LE-SR	U.S. Army's Launched Effects Short Range Effort
MOSA	Modular Open Systems Approach
OPE	Operational preparation of the environment
PLA	People's Liberation Army
PRC	People's Republic of China
SEAD	Suppression of enemy air defenses
SIGINT	Signals intelligence
SLOCs	Sea lines of communication
SOF	Special operations forces
STOL	Short takeoff and landing
SUAS	Small unmanned aircraft system
UAS	Unmanned aircraft system
UGV	Unmanned ground vehicle
USV	Unmanned surface vehicle
UUV	Unmanned underwater vehicle

Executive Summary

Modern battle networks make traditional military mass formations more vulnerable in offensive operations. The use of cheap sensors, drones, electronic warfare (EW), and long-range fires has made it easier for an adversary to detect, target, and destroy ground forces marshalling in assembly areas, capital ships sailing in the open ocean, and waves of high-value aircraft moving into position. However, warfighting still requires the massing of physical forces and non-kinetic effects in different domains in phases and at specific times and spaces to accomplish a mission. There is still a rhythm to battle. The central operational question has become: How does a modern military create mass without becoming a target? What are new theories of victory when proliferated drones and a transparent battlefield define the character of war?

This report defines “mass” as the ability to concentrate enough effects at the right time and place to overwhelm an adversary’s system. In the past, mass meant concentrating troops, ships, or aircraft often at a decisive point to gain an advantage. In the emerging operating environment, mass increasingly means converging multiple distributed, low-cost networked effects in pulsing waves. There are rarely single decisive points or individual blows that upset the military balance. Mass has become the ability to create operational effect without physically concentrating the force to create advantages in time, space, forces, and options. This approach requires developing a new operational art for swarming.

Figure 1: Converging Effects Without Concentrating the Force



Source: CSIS Futures Lab.

This report argues that swarms can restore the offense in modern war. These formations represent a new approach to generating mass that combines low-cost, converging precision effects with disorientation. Swarms are more than a large salvo or a collection of drones. Their power lies in the network and adaption. A swarm can sense, share information, deceive, jam, strike, assess, and reattack as the enemy adapts. It is a complex system in which the sum total of low-cost, modular drones is worth more than the individual parts.

A swarm's value lies in making the adversary's battle network less reliable and unable to adjust to new attack vectors. Decoys, electronic attacks, and loitering munitions force a defender to waste interceptors, reveal hidden sensors, misallocate reserves, and lose confidence in what it sees. The resulting disorientation takes advantage of the friction and uncertainty inherent in war to increase the probability the enemy will make increasingly bad decisions. The result is a form of maneuver warfare that keeps the enemy off balance and on the horns of a dilemma.

Based on this core concept, this report proposes a three-part operational framework for employing swarms in future military operations:

1. **Set conditions.** A swarming formation must map the physical, electromagnetic (EM), and informational environment while also gaining access, positioning launch and sustainment nodes, and shaping the enemy's expectations through deception. The formation must be staged and in position to act.
2. **Pulse.** Swarms should be task organized to deliver a synchronized pulse of kinetic and non-kinetic strikes to reveal vulnerabilities, saturate critical enemy nodes, and create tempo. The formation attacks in waves to maximize confusion.

3. **Consolidate and transition.** Following the pulse, the swarm must assess effects, reload, reposition, and determine whether to exploit or transition to defense. The formation must be able to quickly shift to consolidate gains, exploit success, and reduce the enemy's time to react.

This framework provides a blueprint for deeper experimentation in the coming years. From drones to low-cost cruise missiles operating as part of a larger networked attack, industry can sell the military swarming capabilities, but the operational form only emerges through iteration and continuous refinement based on after-action reviews, concept development, and wargaming inside the profession of arms. The U.S. military must develop new tactics and operational approaches for swarming. The professional must stand in the middle of the swarm and direct it, as opposed to waiting for industry to guide them.

This report explores a new operational framework for swarming using three hypothetical operational cases: U.S. and allied operations against Russia in Kaliningrad, countering China in the South China Sea, and defending against Russia in the Baltics. In the Kaliningrad scenario, when countering Russian defensive networks, swarms help disrupt an integrated air and missile defense (IAMD) network by forcing sensors to radiate, saturating fire-control channels, attacking command nodes, and opening a temporary corridor for follow-on air and missile operations. In the South China Sea, swarms support counter-sea control operations by expanding allied scouting, creating false contacts, disrupting People's Republic of China (PRC) targeting networks, and creating temporary maritime windows without relying solely on large surface combatants or deep mainland strikes. In the Baltics, on NATO's eastern flank, swarms break Russian defense in depth by finding seams, disrupting drone and artillery networks, attacking logistics and command nodes, and protecting the breach against counterattack.

These cases point to a larger policy conclusion. Swarms and launched effects (LE) are part of a joint operational system and, as such, should not be treated as niche munitions or isolated platform experiments. They must be seen as part of a system that includes production, modular open-systems architecture, data rights, access agreements, prepositioned stocks, partner interoperability, training pipelines, and even entirely new planning processes. Seen in this light, efforts to build larger, institutional structures such as the Defense Autonomous Warfare Group (DAWG) and Direct Reporting Portfolio Manager for Unmanned Systems (DRPM-UxS) and to fast-track drone purchases and integration will only work to the extent that they are accompanied by joint and service doctrine initiatives, including testing entirely new formations.¹ This report is an attempt to catalyze those efforts and create the type of logic and grammar required to employ swarms on the battlefield.

The operational logic in this report also highlights key force design implications. The United States should buy launched effects and related swarm systems in operationally meaningful numbers and develop formations trained to generate repeated pulses under combat conditions. To build a deep enough magazine, the United States should also set conditions for a more dynamic and adaptive defense industrial base capable of building swarming systems and making rapid adjustments as conditions change. That requires common platforms and components that support multiple

vendors, developing a rapid software update pipeline, and ensuring a distributed sustainment and repair capacity.

Resourcing is only part of the answer. The critical question is whether the joint force can develop an operational system, including doctrine for launching, sustaining, commanding, and integrating drones with allies in wartime. That will likely require new formations and operating concepts, and it will require congressional oversight to ensure each service does not fall back on bad habits and parochial interests.

There is also a new premium on adaptation. Given the open system architecture and low costs, swarms are likely subject to more rapid battlefield adaptation and counter-adaptation cycles. This dynamic creates a requirement to build learning organizations around easy-to-modify systems. Each successive swarm may use different attack vectors, frequencies, and tactics than the last, creating a need for highly trained military personnel, mission command, and flexible systems.

Key Takeaways

1. Mass still matters in war, but modern military formations must generate it through swarms consisting of distributed, low-cost, hard-to-target systems.
2. This new approach to mass puts a premium on disorienting an adversary's sensors, command systems, and decision cycle.
3. Effective swarming requires a sequence of actions: Set conditions, pulse, and then consolidate and transition before the defender recovers.
4. Launched effects are one practical path to fielding affordable mass and swarms, but they require open architecture, software agility, and coalition interoperability.
5. The United States needs new concepts of operations, dedicated swarming units, career fields, joint task force concepts, and recurring tests that measure whether swarms can regenerate combat power after first contact.

Introduction

The proliferation of cheap sensors and drones has reduced the cost of targeting in multiple domains. What can be seen can be hit. What can be hit can be destroyed. Military forces can now find targets more quickly and strike them more accurately at lower cost. Precision strike is no longer reserved for wealthy nations or confined to operational fires and strategic attacks.² Examples abound, such as the use of drones and loitering munitions in the Middle East and war in Ukraine, civil conflicts raging across the Sahel and Horn of Africa, and speculation

Figure 2: A U.S. Army Soldier Operates a Low-Cost Drone



Source: Staff Sgt. Michael Schwenk/U.S. Army National Guard.

about future People's Liberation Army (PLA) campaigns to compel Taiwan.³ The logic of war remains, though the grammar has changed.⁴

Low-cost precision favors the defense. Creating anti-access/area denial (A2/AD) bubbles that blend terrestrial and space-based sensors with anti-ship, anti-air, and land-attack missiles to keep enemy forces away from a region and entry costly has become easier due to growing access to cheap, networked drones.⁵ As the war in Ukraine illustrates, there is a new “no man’s land” that blends old-fashioned trenches with modern battle networks that integrate sensor grids, EW, and overlapping drone, direct, and indirect artillery fires. Breaking

this defense increasingly requires a concentration of effects in time and space. This is both old and new. The principles of mass and objective are timeless, even as emerging technologies change the economics of war.⁶

The principles of mass and objective are timeless, even as emerging technologies change the economics of war.

Historically, defense has enjoyed cost advantages over offense in war.⁷ This remains the case in 2026, as modern battle networks that integrate multiple combinations of sensors and shooters across domains raise the costs of offensive operations and amplify the asymmetry. Under constant observation and skirmishing attacks, large formations struggle to move into position and launch offensive operations.

Further evidence of the changing character of modern warfare is the fact that long-range precision strike capability has become insufficient to achieve victory. It was not expensive, stealthy cruise missiles that denied Russia sea control of the Black Sea.⁸ It was low-cost sea drones operating as part of a larger network using over-the-horizon kill webs.⁹ In 2024, Ukraine made a surprising breakthrough into Russia's Kursk region. Its forces combined deception and the probing of enemy lines to identify gaps in Russian defenses using a mix of small drones and infiltration by special forces. These efforts supported a series of intermittent pulse attacks that combined effects across the physical, information, and human dimensions.¹⁰

More recently, Israel's 2025 success against Iran in Operation Rising Lion integrated small drones and special mission teams firing non-line-of-sight missiles from the ground to shock the system.¹¹ Though stealth aircraft—waves of F-35I fighters setting conditions for follow-on strikes—were a necessary precondition for breaking Iran's IAMD network, they were insufficient by themselves.¹² This perspective has significant implications for emerging warfighting concepts linked to ideas such as multidomain pulse operations (i.e., Joint All-Domain Operations) that prevail in U.S. defense planning.¹³ These high-end, often theater-level attacks are unlikely to be successful if they do not also integrate low-end swarms (i.e., cheap and attritable mass formations) acting as twenty-first-century skirmishers setting conditions, generating tempo, and helping the larger joint force avoid culmination.¹⁴

As a result, breaking modern battle networks requires precision mass and swarms that stimulate sensor grids, serve as decoys, and overwhelm the defense as means of setting the conditions required for successful follow-on strike packages and joint combined arms maneuver. This idea is at the heart of concepts such as mosaic warfare, Project Replicator, and Admiral Samuel Paparo's call for an "unmanned hellscape" in the Taiwan Strait.¹⁵ This report aims to provide operational depictions that describe how swarms can overwhelm adversary A2/AD bubbles, from the land to the sea, to set conditions for follow-on attacks and maneuver. In other words, the following pages explore the operational art of swarming.

This report describes operational vignettes for how to employ swarms to restore the initiative on the modern battlefield. It uses comparative analysis of three hypothetical modern joint operations to outline critical requirements for successfully employing these formations. Two major insights emerge from the analysis.

First, pulsing drone attacks are effective when they are low cost and work alongside converging information warfare efforts to deceive, manipulate, and deny adversary intelligence and decisionmaking systems. That is, pulsed drone attacks disorient the adversary.¹⁶ That requires a scale that reduces the premium of one-off, exquisite munitions. All things being equal, a swarm that costs as much as a single expensive missile is likely more cost effective, as its pulsing attack waves affect the larger command system.

Second, swarms can achieve campaign-level objectives when they are accompanied by deliberate planning, including operational preparation of the environment (OPE), force deployment and closure, and the building of flexible battle networks that support constant tactical adaption.¹⁷ Swarming is rarely ad hoc, so the lure of autonomy may be overstated. There will still need to be commanders, planners, targeteers, logisticians, and information specialists of multiple flavors, such as EW, signals intelligence (SIGINT), and psychological operations, to properly execute a swarming attack. Even if the terminal phase is autonomous, the larger concept of operations requires military professionals to visualize, describe, and direct combat operations.

The report proceeds as follows. First, it situates and evaluates a critical military trend changing the character of war: the rise of low-cost, modular swarms that can adapt to changing mission parameters. Second, it analyzes how swarms can enable offensive operations through three hypothetical case studies: (1) supporting the suppression of enemy air defense; (2) countering integrated sea control; and (3) breaking a defense in depth in a ground campaign. These three case studies examine Kaliningrad, the South China Sea, and NATO's eastern flank, respectively. While hypothetical, the case studies facilitate visualizing and describing swarming in different operational contexts and allowed the researchers to test the robustness of the concept across domains and threats. The study concludes by considering what conceptual and capability gaps exist across the services to enable deeper integration of multidomain swarms in the U.S. military.

What Is a Swarm?

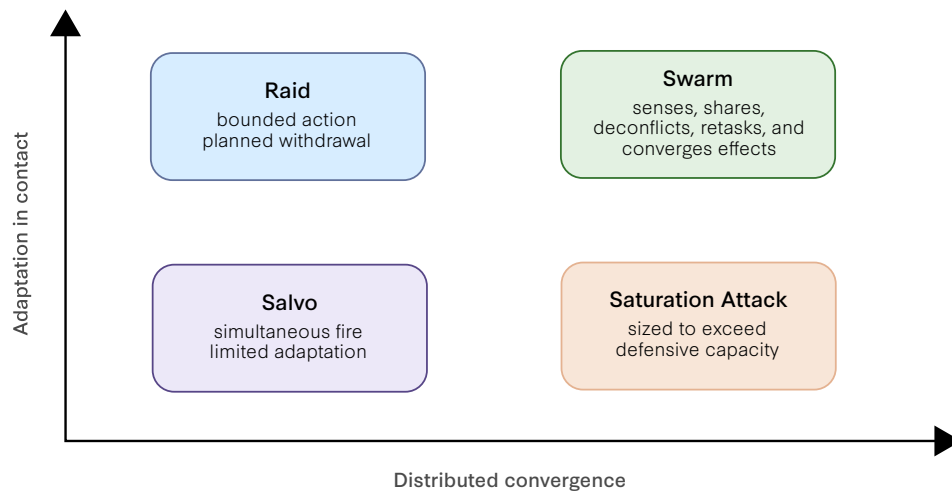
In this report, a “swarm” refers to a network of many low-cost systems that can sense, share information, adapt, and converge effects. Most modern discussions of swarming center on debates about the viability of the Pentagon's Project Replicator and Ukrainian calls to build a million drones a year.¹⁸

These ideas are premised on the assumption that precision mass can be applied in such a way that low-cost semi-autonomous systems overwhelm the adversary.¹⁹ In Replicator, low-cost drones deny China the ability to establish key lodgments in support of a Joint Island Landing Campaign designed to topple the democratically elected government in Taiwan.²⁰ To defend against this amphibious operation, a variety of drones attack Chinese landing craft to create chaos that complicates

operational timelines and buys time and space for Taiwan, and its partners, to counterattack isolated landing forces. Simultaneously, there are emerging reports that China is investing in drone swarms to support offensive military operations against Taiwan.²¹ The envisioned Chinese offensive swarm overwhelms Taiwanese defenders and supports advancing amphibious forces seeking to seize key terrain. In Ukraine, though still nascent, there are already signs of new groups of drones communicating with each other and making independent decisions, thus allowing Kyiv to make up for its lack of manpower to cover defensive fighting positions.²²

A modern swarming attack by drones is not reducible to the limited means and aims of a single salvo, saturation attack, or raid. A salvo denotes simultaneous fire, while a saturation attack is any strike package sized to exceed defensive capacity. A raid, though often more involved than salvos or saturation attacks, remains a bounded offensive action with a limited objective and a planned withdrawal. Crucially, a swarm is able to change its behavior as it learns from the fight. A swarm senses, shares, deconflicts, and adapts in contact with limited human interaction. It relies on tempo, disorientation, and synchronization. To date, most battlefield drone masses have been coordinated stacks rather than true autonomous swarms.²³ Human operators, software links, and ad hoc networks often synchronize swarms, as opposed to benefiting from emergent collective behavior at machine speed.

Figure 3: A Swarm Is More than a Large Salvo



Source: CSIS Futures Lab.

The concept of swarming is not new. Traditionally, swarming refers to “engaging an adversary from all directions simultaneously, either with fire or in force” in a distributed manner, but with converging effects that rapidly and repeatedly overwhelm the target via continuous pulses.²⁴ Swarming can be physical and lethal as well as cognitive and non-lethal. Horse archers pulsing forward to fire volleys of arrows both killed and confused, creating a compounding cycle of fear often as important as the initial casualties. The old idea is to attack from many directions so the enemy cannot tell where the main danger is. As an approach to warfare, swarming achieves a position of relative advantage by surrounding an adversary, thereby leading to confusion, delays, and reduced ability to respond.

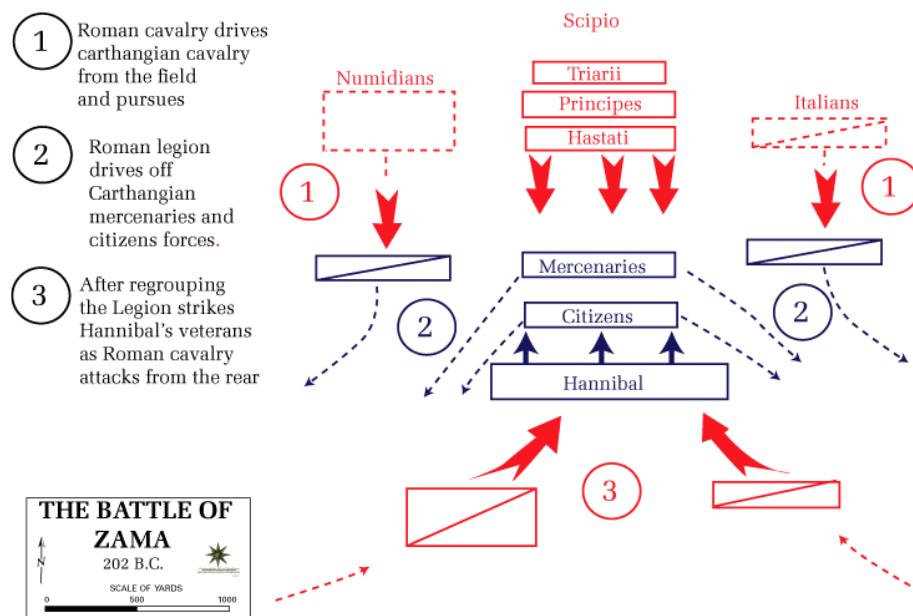
Swarms aggregate and disaggregate to place the enemy on the horns of a dilemma, resulting in leaders fearing the next blow and thereby diminishing their freedom of action.²⁵

Swarms aggregate and disaggregate to place the enemy on the horns of a dilemma, resulting in leaders fearing the next blow and thereby diminishing their freedom of action.

What has changed is technology. Increased lethality drives practitioners to search for new ways to aggregate and disaggregate forces on the modern battlefield. For example, the First and Second Offsets—nuclear weapons and precision strike, respectively—produced distinct military problems related to survivability, mobility, and dispersion on the modern battlefield.²⁶ The First Offset drove a quest to develop battle groups that could disperse to survive a nuclear blast and aggregate for decisive battle.²⁷ The Second Offset and precision strike created similar problems in massing on the battlefield. Similarly, advances in narrow artificial intelligence (AI) and drone technology—the Third Offset—create challenges for the modern warfighter as it becomes cheaper to identify high-payoff targets and engage them with precision fire.²⁸

The concept of dispersed fire and maneuver is not new, though use of the term has shifted from irregular formations to simultaneous fires and more recently to autonomous systems. Tracing this evolutionary trajectory, the word “swarm” defines the convergence of a small series of distributed fire and maneuver actions into a larger battlefield or operational effect.

Figure 4: Battle of Zama (202 BCE)



Historian George Malleon described Scipio's envelopment and pulse in the Battle of Zama as “swarms.”

Source: Department of History, U.S. Military Academy, via Wikimedia Commons.

As seen in Figure 4 above, late nineteenth- and early twentieth-century usage saw swarms as referring to irregular cavalry and militia formations as well as to attacks that seemed to lack organization. In his 1896 seminal work on colonial warfare and insurgency, British Army officer Charles Callwell described multiple forces, including Zulu tribesmen and Afghan formations, as “a great irregular swarm without military formation.”²⁹ In other accounts, the concept also implied a degree of momentum in which changing conditions altered the balance of forces by drawing irregular actors into conventional formations. Describing the 202 BCE Battle of Zama, researchers depict Scipio’s mix of irregular cavalry and skirmishers as swarms.³⁰ In his depiction of the 1422 Siege of Constantinople, Bengal Army officer George Malleison used the term swarm to describe how bribes and propaganda mobilized irregular combatants who “swarmed into the vicinity.”³¹

In the early 1990s, largely in response to the U.S. Department of Defense’s 1992 report about an anticipated military-technical revolution—*Revolution in Military Affairs*—service studies began to look at swarming as the simultaneous application of fires. According to a study by the U.S. Army Training and Doctrine Command in 1994:

... recent U.S. operations show that deep battle has advanced beyond the concept of attacking the enemy’s follow-on forces in a sequenced approach to shape the close battle to one of simultaneous attack to stun, then rapidly defeat the enemy. Commanders may place greater emphasis on operational—and/or tactical-level raids—combined with deep strike means—to break up an enemy’s formations from within.³²

This condition led to a need to stress simultaneity in operations:

Advanced forces will possess the capability to achieve multiple operational objectives nearly simultaneously throughout a theater of operations. This simultaneity, coupled with the pervasive influence of near-real-time military and public communications, will blur and compress the traditional divisions between strategic, operational, and tactical levels of war.³³

As a swarm, network nodes would have varying specialties such as intelligence, surveillance, and reconnaissance (ISR), command and control (C2), and weapons employment. These nodes in turn “share their sensor information, and self-synchronise in order to mass the effect of their weapons.”³⁴ These arrays can be emergent or situationally aware swarms and be discretely organized as hierarchal or distributed.³⁵ A situationally aware swarm “uses networking to fuse sensor information from individual nodes to produce an integrated situational awareness picture, and also to synchronise actions.”³⁶ Most analyses along these lines focus on offensive applications of these systems for fire and maneuver, including extending traditional concepts such as reconnaissance pull, a tactic where intelligence gathered from a wide area identifies enemy weaknesses to guide the main force toward the path of least resistance.³⁷

The concept spread beyond the services. For example, a 2000 RAND study referred to swarm tactics as “small, distributed units and maneuverable fires converg[ing] rapidly on particular targets.”³⁸ The study identified 10 historical cases “in which the scheme of maneuver involved the convergent attack of several (or more) semiautonomous (or autonomous) units on a target force

in some particular place.”³⁹ The cases in turn reflected two broad categories of swarming: massed (e.g., swarming army masses and then dispersing as the tactical situation changes) and dispersed (e.g., traditionally guerrilla tactics in which dispersed units converge).

Studies of effects-based operations similarly emphasized swarming as aggregating dispersed fire and maneuver elements. In the early 2000s, the Israel Defense Forces (IDF) advocated for “coordinated attacks from different directions by small, dispersed, and networked units.”⁴⁰ Observers of the 2006 IDF campaign against Hezbollah in southern Lebanon used the term swarming to describe Hezbollah’s anti-armor ambush tactics, in which small teams fired multiple anti-tank missiles simultaneously and then displaced to defensive positions.⁴¹

This cursory historical overview not only demonstrates that the concept of swarming is neither new nor novel but also offers insights into what swarming entails. First, swarms are not necessarily a byproduct of linear systems nor singularly offensive. Skirmishers of old could swarm in the defense to delay an adversary advance and use feints to misdirect the enemy. This idea finds parallels in biology, where complex systems routinely swarm in the defense. For example, many natural swarms confuse predators, making it harder for a predator to single out and pursue one individual target, even if the swarm as a whole is not spared from attack. This dynamic is most vividly seen in the dense, rolling “bait balls” formed by schools of fish as they swarm to confuse predators.⁴²

Swarms offer a means of confusing, even paralyzing, an attacker. Disorientation, as much as destruction, is the goal. Swarms are thus not only offensive tools; their capability to confuse attackers makes them effective defensive tools as well.

Second, war may not be a linear system where inputs equal outputs.⁴³ A 1996 study sponsored by Lieutenant General Paul Van Riper, then commanding general of U.S. Marine Corps Combat Development Command, argued that “land combat is a complex adaptive system.”⁴⁴ To model land warfare, the research used SWARM, a multi-agent software platform developed by the Santa

Figure 5: Small Fish in a Bait Ball (Defensive Swarm) Formation



Source: Andrea Izzotti/Adobe Stock.

Fe Institute that simulates complex adaptive systems.⁴⁵ In the 1996 study’s models, the simultaneous application of fire and maneuver implied a non-linear system with cascading effects. In other words, it demonstrated that small inputs can produce larger, cascading outputs. Swarms create more opportunities for realizing these non-linear gains.

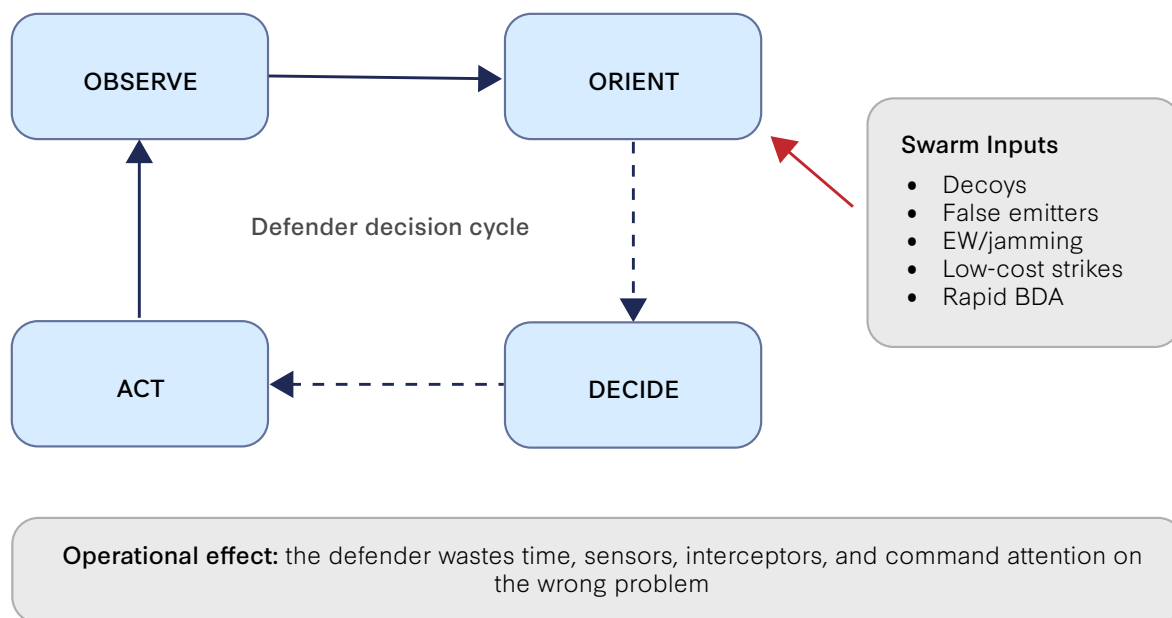
Third, while tactical action on land is the heart of war, swarms can generate operational-level effects that extend well beyond the land domain. Future studies therefore must explore the operational art of swarming across air, sea, space, and cyberspace. Specifically, research must examine swarming as a non-linear threat

where synchronized, decentralized actions cascade to create effects far greater than the sum of their parts. These efforts should encompass offense, defense, and deception.

Swarms offer a means of confusing, even paralyzing, an attacker. Disorientation, as much as destruction, is the goal.

In this respect, swarming is related to an emerging defeat mechanism in modern war: disorientation.⁴⁶ The concept of disorientation entails making the enemy unsure about what is real, what matters, and where to respond. The concept goes beyond the fog of war to propose creating a condition in which an adversary cannot orient themselves, creating paralysis and increasing the probability that they undertake self-defeating and costly actions.

Figure 6: Disorientation as a Defeat Mechanism: Undermining the Defender Decision Cycle



Source: CSIS Futures Lab.

The swarm attacks the enemy's ability to interpret events. False signals, decoys, and sporadic strikes on the edge of the battlefield make the defender spend time confirming what is real and eliminating what is not. That delay creates the opening for the next attack. In effect, the convergence of deception, information warfare, and swarming with low-cost drones from multiple directions attacks sensor feedback loops. By injecting "noise" into the enemy's observation channels, a swarming force corrupts the orientation phase of the observe, orient, decide, act loop to create mismatches between perception and tactical reality.⁴⁷ This forces the enemy to turn inward, paralyzing their ability to coordinate a response as they struggle to verify a flood of contradictory

data. This results in a *destructive* positive feedback loop: The enemy commits resources to false indicators, receives validation from their sensors that they are “engaging” targets, and consequently doubles down on a flawed course of action, thereby accelerating their own collapse. In this new grammar of warfare, disorientation simultaneously attacks the enemy’s physical disposition and cognitive orientation, ensuring that by the time they discern a true threat from fabrication, the window for effective tactical action has closed.

Operationalizing this concept relies on the deployment of low-cost, modular swarms that place the adversary on the horns of a dilemma. Flexibility is key to compounding adversary fear and diluting their decisionmaking. The enemy should have to imagine multiple attack vectors. Rather than a single massed formation, these distributed networks create a “ghost landscape” where cheap decoys and electronic emitters mimic high-value targets, compelling the enemy to radiate their sensors and reveal their positions in order to differentiate true versus false data. Decoys and false signals can make the defender waste time, attention, and ammunition on the wrong targets.

Swarms enable the weaponization of analysis paralysis by intentionally creating too much data for the adversary to effectively manage within the narrow time constraints of conflict decisionmaking.

This process weaponizes the noise-to-signal ratio: While the defender exhausts expensive interceptors and cognitive bandwidth chasing phantoms, they create the very temporal and spatial gaps that the attacking force intends to exploit. More than overwhelm, the swarm

Figure 7: Low-Cost Drones in Ukraine



Two Ukrainian soldiers using a quadcopter drone.

Source: Serhii Mykhalchuk/Global Images Ukraine via Getty Images.

manipulates the enemy’s feedback loops, causing them to misallocate resources against non-existent threats while the true precision pulse strikes the exposed seams of their defense. In effect, swarms enable the weaponization of analysis paralysis by intentionally creating too much data for the adversary to effectively manage within the narrow time constraints of conflict decisionmaking.

At the tactical edge, this disorientation is physically enabled by small, fast, and increasingly autonomous systems that defy traditional countermeasures. First-person-view (FPV) drones and loitering munitions, flying at extremely low altitudes, utilize terrain

masking to blend into ground clutter, effectively vanishing from the view of radars designed for larger, faster aircraft.⁴⁸ Furthermore, the integration of fiber-optic tethers and automated terminal guidance fundamentally alters the survivability calculus. These systems are immune to the EM jamming that increasingly forms the backbone of modern defense.⁴⁹ Too small for conventional missile interceptors and effectively invisible to EW, swarms bypass the enemy's defenses to strike high-value targets, all the while intentionally creating chaos and confusion. Small drones can be hard to detect, hard to jam, and cheap to replace.

The air littoral is key for launching these attacks.⁵⁰ The air littoral refers to the dense, highly cluttered airspace extending from the Earth's surface up to approximately 10,000 feet, but often much lower.⁵¹ It is the transition zone between ground forces and "blue skies" where aircraft operate. Often, this low-altitude airspace is where drones and helicopters can maneuver, including using terrain masking and clutter to conceal their approach.

For offensive swarming, the air littoral is the primary avenue of approach. Even when motherships deploying launched effects operate at much higher, standoff altitudes to maximize range and survivability, the swarm's terminal maneuver occurs entirely within the air littoral. When launched from the ground, and operating within the clutter of the battlefield and utilizing terrain masking (e.g., hiding behind tree lines, hills, and urban canyons) an offensive swarm flies beneath the radar horizons of legacy IAMD networks. The swarm can get close and then use false emitters to saturate enemy sensors, blinding early warning systems and overwhelming local point defenses to break down A2/AD bastions.⁵²

Launched Effects

Drones operating in the air littoral can be launched from air-, ground-, or sea-based platforms. Increasingly, industry and military concepts refer to this versatility as launched effects and use the idea to drive capability development optimized for swarming. General Atomics Aeronautical Systems, Inc. (GA-ASI) produces the Advanced Air-Launched Effects (A2LE) as an additively manufactured capability launched from the internal bay of the MQ-20 Avenger unmanned aircraft system (UAS). The system is part of a larger effort to explore low-cost, modular air-launched effects for future “mothership” concepts.⁵³ In an initial series of Avenger flight tests, GA-ASI validated both captive carry and clean separation of the A2LE from the Avenger’s internal weapons bay, proving the basic launched effects deployment concept. In a subsequent demonstration at Dugway Proving Ground reported in early 2024, GA-ASI and its partner Divergent successfully flew a fully 3D-printed A2LE produced with the Divergent Adaptive Production System, adding release, flight, and recovery to its concept of low-cost, mass-manufacturable architecture.⁵⁴

Figure 8: General Atomics' A2LE Launches from MQ-20 Avenger UAS



Source: GA-ASI.

General Atomics also produces the Enhanced Air and Ground Launch Effect Technology (Eaglet). This system is part of the U.S. Army's "LE Large" category, designed to be launched from a Gray Eagle Extended Range UAS, rotary-wing aircraft, or ground vehicles.⁵⁵ Eaglet's first flight took place on December 8, 2022, at Dugway Proving Ground, when a U.S. Army MQ-1C Gray Eagle Extended Range UAS released the launch effect in a jointly funded demonstration with the Army Combat Capabilities Development Command, Army Research Laboratory (DEVCOM ARL) and the Aviation and Missile Center (AvMC), validating captive carry and safe separation.⁵⁶

Table 1: GA-ASI Eaglet Key Characteristics

System	Weight	Wingspan	Speed	Payload	Range	Endurance
GA-ASI Eaglet	<200 lb	10.5 ft	115 kt	20-30 lb	~435 miles	~8 hours

Source: Stefano D'Urso, "General Atomics Tests New Eaglet Air Launched Effect," The Aviationist, February 17, 2023, <https://theaviationist.com/2023/02/17/general-atomics-tests-new-eaglet-air-launched-effect/>.

The Gray Eagle can carry the lightweight (less than 200 lb) Eaglet "for thousands of kilometers" before launch, enabling standoff carriage with stand-in effects at the edge of contested airspace.⁵⁷ The MQ-1C Gray Eagle (Extended Range), which successfully carried out tests launching the Eaglet, should be able to carry up to three Eaglets at once, with two on wing stations and one on the centerline station, according to publicly available payload capacity figures.⁵⁸ A GA-ASI spokesperson mentioned a potential capacity to carry four Eaglets simultaneously.⁵⁹ To date, the only public Eaglet launch test involved a single Eaglet launched from a wing station.

Figure 9: GA-ASI Rendering of Eaglet Launch from Gray Eagle UAS



Source: GA-ASI.

GA-ASI also produces the Sparrowhawk, a multi-mission, recoverable small UAS (SUAS) that deploys from the wing of larger unmanned aircraft such as the MQ-9 Reaper or the MQ-9B SkyGuardian and can be recovered in mid-flight.⁶⁰ It provides ISR, SIGINT/ELINT (electronic intelligence), and jamming in a compact airframe optimized for contested environments.⁶¹

Table 2: GA-ASI Sparrowhawk Key Characteristics

System	Weight	Wingspan	Speed	Payload	Range	Endurance
GA-ASI Sparrowhawk	500 lb	14 ft	80 kt cruise, 150 kt dash	60 lb including SIGINT, jammers, electro-optical/infrared, and high explosives	575 miles	>10 hours

Source: “Sparrowhawk,” GA-ASI, accessed March 10, 2026, <https://www.ga-asi.com/remotely-piloted-aircraft/sparrowhawk>.

Initial captive-carry tests in September 2020 flew a Sparrowhawk on an MQ-9A as an airborne launch and recovery demonstrator for the Advanced Battle Management System “attributableONE” effort, controlled via GA-ASI’s Metis software-defined, laptop-based control station and networked over the meshONE data link with the CODE autonomy engine to explore collaborative autonomy in denied environments. GA-ASI highlighted that Sparrowhawk enables below-the-weather ISR, attributable ISR/EW in contested airspace, extended MQ-9 sensor reach, and distributed sensors across the battlespace while keeping the mothership at a safer standoff distance.⁶² Follow-on testing of an aerial recovery system from the MQ-20 Avenger using a hoist-deployed towline

is intended to allow motherships to launch and then recapture Sparrowhawk-type SUAS and launched effects in mid-air, supporting a concept of long-endurance Reaper/Avenger “command nodes” forward-deploying recoverable small drones for ISR, EW, and suppression of enemy air defenses (SEAD) support in highly contested environments.⁶³

Figure 10: GA-ASI Rendering of Sparrowhawk SUAS



Source: GA-ASI.

RTX-owned Raytheon produces the Coyote, a reusable, multi-mission (i.e., kinetic and non-kinetic) counter-UAS (C-UAS) interceptor and launched effects solution. The firm describes Coyote Block 3NK as an interceptor that can loiter, defeat drone swarms, and then be recalled and redeployed, providing a recoverable “airborne magazine” for swarm defense while minimizing collateral damage.⁶⁴ In February 2026 trials, the Coyote Block 3NK engaged and defeated multiple SUAS in a single exercise, integrating with the KuRFS radar to deliver layered base and force protection.⁶⁵

Figure 11: Raytheon’s Coyote Block 2 (Kinetic C-UAS Effector) Launching from the U.S. Army’s Low, Slow, Small Unmanned Aircraft Integrated Defeat System (LIDS)



Source: Raytheon.

In addition, RTX markets Coyote launched effects variants for reconnaissance, surveillance, target acquisition, EW, precision strike, and communications relay, extending beyond-line-of-sight sensing and effects for U.S. and allied forces.⁶⁶ The Coyote Block 3 was one of three systems (with AEVEX’s Atlas Group II and Anduril’s ALTIUS-600) chosen for the U.S. Army’s Launched Effects-Short Range (LE-SR) special user demonstration in August 2025.⁶⁷ The Army’s LE-SR program was for launched effects with a range of 40-125 km.⁶⁸

Anduril’s ALTIUS-600 is an autonomous air vehicle in the ALTIUS family, designed as an air-launched effect for multi-mission ISR, SIGINT, EW, radio frequency decoy, communications relay, and cyber roles.⁶⁹

Table 3: Anduril ALTIUS-600 Key Characteristics

System	Weight	Wingspan	Speed	Payload	Range	Endurance
Anduril ALTIUS-600	27 lb	8.3 ft	60 kt cruise, 90 kt dash	7 lb nose payload	230 miles	3.5 hours

Source: “Altius,” Anduril, accessed March 10, 2026, <https://www.anduril.com/altius>.

The modular nose bay supports swappable payloads, ranging from ISR/SIGINT/EW and C-UAS jammers to a high-explosive or shaped-charge warhead, and the airframe is designed to be recoverable when configured for non-kinetic missions.

Figure 12: Launch of Anduril's ALTIUS-600



Source: TWZ.

Figure 13: Launch of an ALTIUS-600 by UH-60 Black Hawk Helicopter



Source: U.S. Army.

Demonstrations documented by Army and Air Force sources have shown ALTIUS-600 tube-launched from UH-60 Black Hawks and MQ-1C Gray Eagles at Yuma Proving Ground, from C-130-class aircraft and maritime/ground launchers, and from XQ-58A Valkyries and MQ-9 Reapers as part of Air Force Research Laboratory and Air Force Special Operations Command’s Adaptive Airborne Enterprise concept.⁷⁰ The U.S. Army’s LE-SR effort notes that the ALTIUS-600, alongside AEVEX’s Atlas, was selected for the initial LE-SR fielding after a special user demonstration, with PEO Aviation Brigadier General David Phillips emphasizing both systems were “production-ready” and could be rapidly fielded.⁷¹ ALTIUS-600 is one of four closely related variants (ALTIUS-600, ALTIUS-600M, ALTIUS-700, and ALTIUS-700M) built on a common autonomous air vehicle architecture.⁷²

AEVEX’s Atlas Group II Launched Effect is a lightweight, short-range launched effect selected by the Army for its initial LE-SR fielding effort in 2025, following soldier test events and a special user demonstration.⁷³

Table 4: AEVEX Atlas Key Characteristics

System	Weight	Wingspan	Speed	Payload	Range	Endurance
AEVEX Atlas	36.5 lb	75.5 in	65 kt cruise, 80+ kt dash	7.5 lb kinetic or ISR payload	80+ miles	70+ minutes

Source: “Atlas,” AEVEX, <https://aevex.com/unmanned-systems/precision-strike-systems/atlas/>.

Designed as a precision strike platform, Atlas provides 70+ minutes of endurance, 70+ nautical miles (~130 km) of range, a 65 kt cruise (80+ kt dash), and a 7.5 lb kinetic or ISR payload, packaged in a 36.5 lb man-portable airframe.⁷⁴ Its modular architecture supports kinetic and ISR payloads, with mesh networking, swarm autonomy, and visual-based assured positioning, navigation, and timing to enable GPS-denied operations that a small team can launch and control with minimal setup.⁷⁵ According to PEO Aviation Brigadier General David Phillips, similar to Anduril’s ALTIUS-600, Atlas was chosen because it was “production-ready” and could be rapidly fielded, making it suitable for near-term operational deployment as the Army’s first operational LE-SR capability.⁷⁶ The Army intends to field launched effects such as Atlas across active-duty divisions by the end of FY 2026, aligning LE-SR with broader modernization priorities.⁷⁷

Figure 14: AEVEX's Atlas Precision Strike System



Source: AEVEX.

Furthermore, additive manufacturing is beginning to reshape the launched effects ecosystem by compressing design cycles, reducing tooling costs, and enabling cheaper airframes and propulsion components for attritable systems. General Atomics' demonstration of a fully 3D-printed A2LE released from the MQ-20 Avenger UAS showed how additive production can speed the path from concept to flight test for modular launched effects bodies.⁷⁸ The Army is pushing the same logic into fuselage production, funding work to 3D print composite drone fuselages that maximize internal volume while reducing weight.⁷⁹ At the propulsion layer, the Air Force's investment in Beehive's 3D-printed Frenzy Engine indicates that the affordable mass problem is now being attacked both in terms of airframe and engine design.⁸⁰ More broadly, recent reporting on battlefield additive manufacturing underscores the operational value of distributed production, repair, and modification closer to the fight.⁸¹

These launched effects offerings are a bid to generate affordable, precision mass in the air littoral.⁸² Precision mass transcends the industrial-age concentration of thousands of localized troops or the more modern massing of large, expensive platforms. Instead, it reflects the ability to converge overwhelming, accurate kinetic and non-kinetic effects from distributed platforms and attack vectors. The purpose is to create the effect of mass without putting a large, easy-to-target force in one place. Because the swarm is geographically dispersed but connected, it achieves the mass required to shatter an enemy's battle network without presenting an easy target to counterattack. This conceptual shift underpins a surge of new Pentagon initiatives aimed at restoring offensive

maneuver. Programs such as the Pentagon's Replicator initiative, the Army's Launched Effects program, and the U.S. Navy's Hedge Strategy all reflect this deliberate force design transition: leveraging scalable, autonomous swarms operating in the air littoral to overwhelm adversary defenses with affordable, precision mass.⁸³

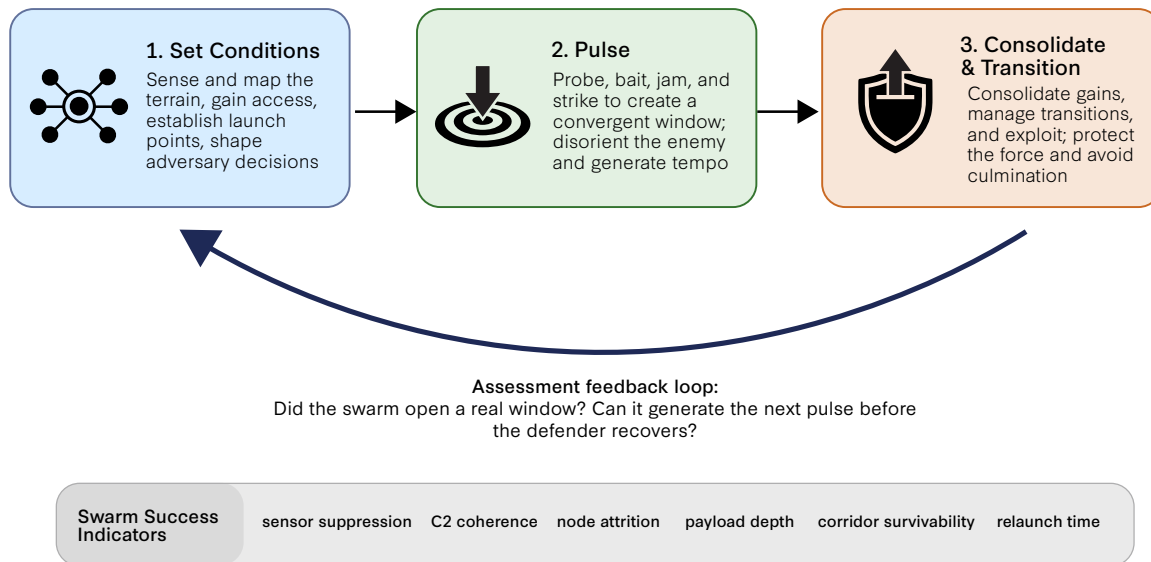
Launched effects can also support other strike packages to maximize disorientation. For example, waves of low-cost launched effects can be launched in tandem with low-cost cruise missiles, creating a layered attack.⁸⁴ They can also be integrated with containerized payloads and new ground-based affordable mass options currently under development to stretch enemy intelligence as they search for where the next attack might come from.⁸⁵ Likewise, launched effects can be used to stimulate sensors, jam key systems, and open strike lanes for more exquisite long-range systems such as Tomahawks, Long Range Anti-Ship Missiles, and Precision Strike Missiles.

Creating an Operational Framework

The promise of new capabilities fails without clear concepts of employment. Translating the theoretical promises of precision mass and air littoral exploitation into battlefield success requires an operational framework that establishes the logic behind swarming operations. This framework should help guide commanders and planners and ensure that swarms are more than disorganized mobs of drones thrown at tactical problems. There needs to be a blueprint for simultaneously surveilling battlespace and applying fires, sharing sensor data, and manipulating how the adversary observes, orients, decides, and acts on the battlefield. Therefore, swarm employment must be orchestrated as a deliberate, phased campaign that systematically unravels the adversary's multi-domain battle networks and creates fleeting windows of localized superiority.

Given this logic, and depicted in Figure 15 below, the ideal sequence for any swarming campaign departs from rigid, attrition-based models focused on force ratios at decisive points and relies instead on a distinct operational framework built around phasing and sequencing: setting conditions, delivering a multi-axis pulse, and rapidly consolidating gains to transition to follow-on exploitation.

Figure 15: Operational Framework for Swarming Operations



Source: CSIS Futures Lab.

First, the force seeking to use swarms to seize the initiative must set the conditions. This includes activities related to getting logistics set, OPE, and mapping the battlespace to provide a baseline operating picture. Put simply, swarms have to move to launch points while planners identify flight routes, potential targets, and how best to disorient the enemy command system.

Second, the swarming force needs to attack, conducting a series of intermittent pulses designed to identify enemy weaknesses and respond to changing conditions. The networked formation needs to probe, bait, and attack enemy vulnerabilities that emerge in the physical, informational, and human dimensions. The goal is to maximize disorientation and take advantage of enemy missteps as they emerge in the chaos of battle.

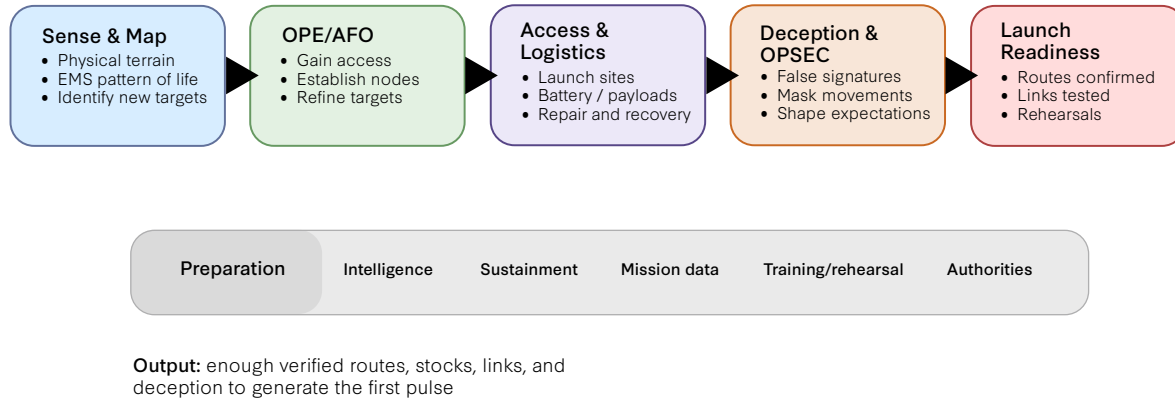
Third, swarms require careful attention to consolidating gains and managing transitions. To avoid culmination, the networked formation needs to reconstitute and determine how far forward to advance its supply lines and when to transition to the defense, follow-on exploitation, or pursuit missions based on enemy counteractions. Each of these phases is detailed below using examples from the 2024 Ukrainian Kursk offensive.⁸⁶

Set Conditions

Setting conditions for a swarming attack consists of deliberate preparation of the environment such that it enables a distributed force to launch convergent, multi-axis pulse attacks. In most swarming concepts, many small, semi-autonomous (or even autonomous) elements converge rapidly on key nodes, then disperse, adapt to new conditions, and reattack. As a result, a successful swarm offensive depends more on sensing, positioning, and sustaining than any single attack. When forces

are not already forward deployed, it also includes deploying and connecting new units into proper C2 and logistics networks to support combat operations.⁸⁷

Figure 16: Build the Swarm Before It Launches



Source: CSIS Futures Lab.

First, there is a need to sense and map the environment. No map is ever complete, just as no intelligence estimate is ever final. Sensing and mapping the environment includes a mix of building on existing estimates and tasking new collection requirements to understand the physical, cognitive, and information dimensions of the battlespace.⁸⁸ These activities typically include updating signal surveys (i.e., how people use the EM environment), mapping information networks (e.g., common social media usage patterns, prevailing themes and narratives, existing internet service providers, and cell providers), and building the architecture required to integrate threat, friendly, and environment information into a common operating picture. What the naked eye can see and physical terrain are only half of the equation. These surveys help establish accurate EM spectrum awareness, identify constraints and interference risks, and anticipate where communications, sensing, navigation, and information warfare effects are likely to be degraded or contested.⁸⁹ They can also include scraping social media to understand public sentiment or unit morale, key narrative themes, and human terrain. This information ensures that the swarm can close a kill web (i.e., integrate comms, pass target-quality tracks, and attack authorities) under real conditions and across dimensions (i.e., physical, human, information).

Mapping also includes analyzing avenues of approach. This includes route planning and building movement options for launch teams, sustainment, recovery, and follow-on forces. Planners, ideally working alongside custom AI agents, validate mobility corridors, identify timing windows that minimize enemy detection, and establish alternative options so tempo does not collapse when a single route, crossing, or node becomes denied.⁹⁰

Next, setting conditions includes OPE.⁹¹ Doctrinally, OPE falls under the broader umbrella of preparation of the environment, which also includes advanced force operations (AFO) and intelligence operations. OPE may involve tasks such as passive observation, area familiarization, and the development of reception infrastructure. In more time-sensitive conditions, these

activities include AFO, a specialized subset of OPE designed to refine the location of specific targets and set the conditions for near-term mission execution.⁹² Unlike general preparation, AFO is time-sensitive and directly supports imminent operations through active tasks such as clandestine target refinement, terminal guidance for incoming strike forces, and the establishment of reception, staging, onward movement, and integration infrastructure.⁹³ In plain terms, OPE and AFO are the advance work that helps a force understand the area, place support, and reduce risk before an operation.

OPE and AFO include logistical preparation and prestaging the equipment required to support swarm generation. Swarms shift “mass” from a few exquisite platforms (e.g., fifth-generation fighter jets and long-range strike assets) launched from large, fixed air bases or capital ships (e.g., carriers) to multiple nodes. The ideal swarm is dispersed yet converges effects in time and space. This requirement increases the demand for forward-positioned energy (e.g., fuel and batteries), munitions and payloads, spare parts, and maintenance kits. Prepositioned stockpiles can help reduce closure times for combat and support forces early in a contingency. Swarm generation depends on how quickly systems can be rearmed, recharged, repaired, and relaunched.⁹⁴ Practically, that means setting conditions includes selecting and preparing staging areas, organizing supplies for rapid movement (often containerized), arranging resupply, and planning sustainment flows so follow-on echelons can arrive and exploit the swarm-created window before it closes.

Last, both OPE and AFO include implementing tactical deception and operational security measures required to mask movement and pull the enemy out of position.⁹⁵ Building on the intelligence activities involved with sensing, military planners identify the best ways and means to support deceiving the enemy and limiting its options for attacking swarming units while they move into position. This includes identifying key conduits and filters that shape how the enemy sees the battlespace.⁹⁶

Winning the fight for information is a violent struggle to see first, understand first, and strike first, effectively dislocating the enemy before the main swarming pulse is even delivered.

In an active combat zone, setting conditions requires dynamic shaping activities that go beyond static planning to include armed reconnaissance missions employing both swarming assets and traditional formations to validate targets and ensure the integrity of the kill web. Possessing a target deck and forward-positioned systems does not guarantee operational success, however. Because war is a complex, adaptive system, the underlying logic of an attack must be continuously tested against enemy responses to ensure that communication links and target-quality tracks remain viable under pressure. Future success depends on the ability to “win the fight for information.”⁹⁷ This involves aggressive reconnaissance and counter-reconnaissance operations to strip the enemy of its situational awareness while preserving one’s own. Winning the fight for information is a violent

struggle to see first, understand first, and strike first, effectively dislocating the enemy before the main swarming pulse is even delivered.

The requirements for extensive intelligence and OPE are missing in the majority of the swarming and unmanned systems discussions, which often tend to highlight exquisite attacks in their terminal phase. The world watches drones destroying tanks and surface-to-air missile launchers without realizing, or even considering, the time and effort it took to move the capabilities into position and identify the best time to strike, much less the planning and mission rehearsals. War is viewed as a single attack in the terminal phase. These oversights are likely why the U.S. military is stalled in its integration of larger unmanned formations and development of new operational concepts.

SETTING CONDITIONS IN KURSK

Ukraine's 2024 offensive into the Russian oblast of Kursk effectively operationalized swarming concepts by employing distributed, semi-autonomous mobile groups that converged on key nodes rather than relying on a single axis of advance. As described in swarming theory, Ukrainian forces initiated a multi-axial "pulse," simultaneously infiltrating the border at several distinct points to overwhelm the decisionmaking capacity of local Russian commanders.⁹⁸ The Ukrainian elements, often comprised of small, armor-supported tactical groups extensively using drones as reconnaissance and strike elements, bypassed strongpoints to strike deeper into the Russian rear, effectively dispersing and reaggregating to encircle settlements such as Sudzha.⁹⁹ This maneuver capability was enabled by the mission command and autonomy granted to lower-level commanders, allowing them to exploit gaps in the Russian defensive network in real time without waiting for centralized direction, a hallmark of successful swarming behavior.¹⁰⁰

This Ukrainian campaign offers several important lessons for swarm employment. First, the operation demonstrates that success relies heavily on achieving information dominance before the first volley. This required not just existing intelligence but active "signal surveys" and mapping of the EM spectrum and information environment. In the weeks preceding the August 2024 operation, Ukrainian forces systematically blinded Russian ISR capabilities along the border using EW to jam Russian communications and drone frequencies.¹⁰¹ This effectively denied Russia the "transparent battlefield" it had been relying on, allowing Ukrainian units to move into position and identify gaps in the Russian defensive network (e.g., lightly manned border posts guarded by conscripts) without generating the signatures that typically precede a major offensive operation.

The OPE and AFO phases were equally critical in the campaign's success, involving both the physical shaping of terrain and the complex logistics of force closure. Ukrainian special operations forces (SOF) reportedly infiltrated the Russian border region as early as August 4, two days prior to the main assault, to conduct close-target reconnaissance and sabotage.¹⁰² These elements worked to neutralize border defenses and clear obstacles, including through the reported use of engineering assets to breach "dragon's teeth" fortifications and minefields that would have otherwise stalled the rapid convergence of the swarm.¹⁰³ Simultaneously, Ukraine secretly massed elements of the 80th and 82nd Air Assault Brigades in the Sumy Oblast. Under the

strict guise of training exercises and defensive rotations in Sumy, planners prepositioned the fuel, munitions, and maintenance assets required to avoid culmination once the attack began.¹⁰⁴ This prepositioning of munitions and fuel allowed for a high-tempo advance 35 km deep into hostile territory, validating that sustainment flows are as critical to swarming success as the combat platforms themselves.¹⁰⁵

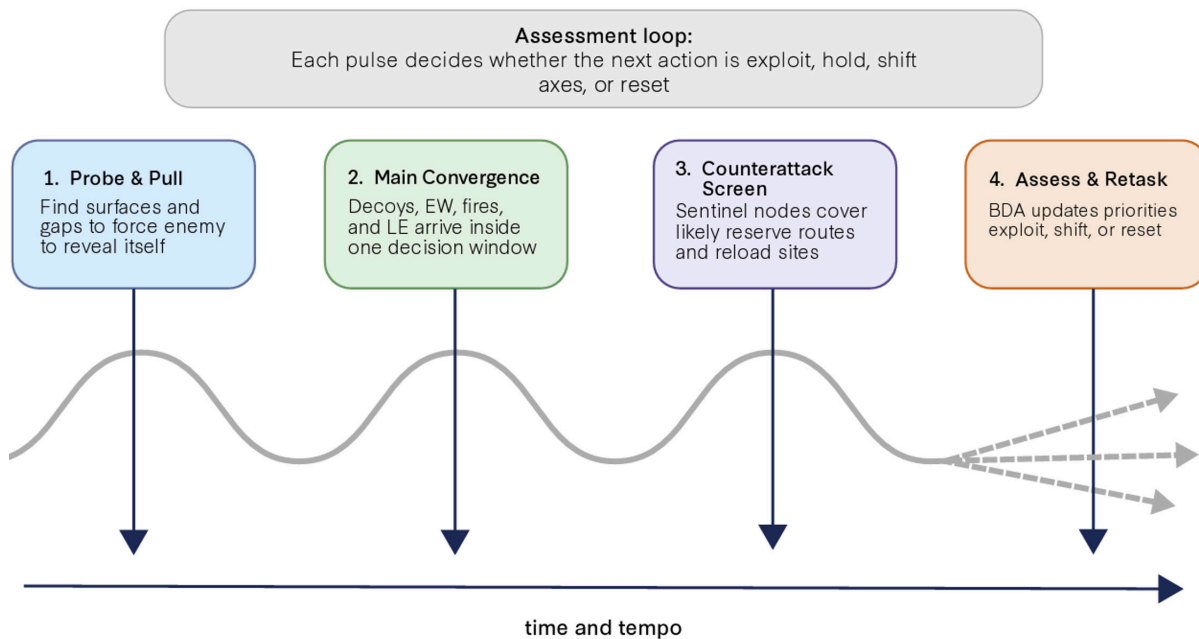
Finally, the Kursk operation established the importance of deception to mask movement and pull the enemy out of position. Planners successfully implemented a regime of strict operational silence and disinformation, framing the massive buildup in Sumy as a combination of a defensive rotation and training exercises rather than as an offensive staging.¹⁰⁶ This narrative leveraged the “cognitive dimension” of the battlespace mentioned in the sensing phase by reinforcing Russian confirmation bias that Ukraine was incapable of large-scale offensive operations. By the time Russian command realized the reality of the situation, Ukrainian units had already penetrated the border. This successfully limited Russia’s options for attacking the swarming units, effectively paralyzing Russia’s decisionmaking cycle during the critical opening hours of the campaign.¹⁰⁷

When the infiltration of Russian lines began, the Ukrainian conventional forces were screened by an EM layer, specifically a dense sensing and striking network that blinded the adversary. Ukrainian forces deployed FPV drones to systematically hunt Russian reconnaissance elements, effectively denying Russia the “transparent battlefield” required to direct its own artillery.¹⁰⁸ By dominating the EM spectrum and jamming Russian communications, Ukrainian units created a localized kill web within which they could pass target-quality tracks to fire support faster than the disjointed Russian units could report them. This allowed the swarming formation to move with impunity, turning the Russian reliance on static defense into a liability as their fixed positions were isolated and bypassed by faster-moving Ukrainian columns.

Pulse

A pulse is a short, coordinated burst of sensing, deception, jamming, and attacking. In the abstract, the swarming attack phase consists of three successive, intermittent pulses. The initial pulse functions as a distributed movement to make contact, designed not to seize terrain immediately but rather to win the fight for information and develop the situation.¹⁰⁹ Utilizing infiltration, semi-autonomous swarm elements (e.g., unmanned systems, EW teams, and light mobile detachments) probe to identify enemy surfaces (strongpoints) and gaps. This aligns with ground warfare tenets such as flexibility, as the force does not adhere to a rigid scheme of maneuver but employs reconnaissance pull instead. When the swarm encounters resistance, it fixes the enemy with fires. When it finds a gap, it signals the network, effectively “pulling” the main body through the path of least resistance.¹¹⁰

Figure 17: Pulses: Short Bursts of Sensing, Deceiving, Jamming, and Striking



Source: CSIS Futures Lab.

Once gaps are identified via the first pulse, the main pulse occurs, characterized by the offensive characteristics of concentration and tempo.¹¹¹ Unlike a traditional linear assault, this pulse features the rapid convergence of dispersed loitering munitions, precision fires, and information effects (e.g., electronic attacks, cyber operations, and influence activities) on the identified weak points, essentially “swarming” effects in the physical, information, and human dimensions simultaneously. This creates a dilemma for the enemy. Perceiving threats from multiple directions, the defender is unable to quickly identify the main attack.¹¹² By bypassing isolated strongpoints to strike deep at command nodes and logistics, the offensive force achieves simultaneity, paralyzing the enemy’s decisionmaking cycle. The objectives comprise physical destruction and, more significantly, the disintegration of the enemy’s defensive integrity, turning a tactical breach into an operational collapse. In this respect, the concept of swarming can be seen as the logical extension of maneuver warfare to the use of unmanned systems.¹¹³

The concept of swarming can be seen as the logical extension of maneuver warfare to the use of unmanned systems.

The third and final pulse anticipates the inevitable counterattack, shifting the form of maneuver from the dispersed offensive aimed at converging effects to a mobile defense or even a hasty ambush conducted by an advanced guard element.¹¹⁴ Recognizing that war is a complex system, this

phase projects force depth well beyond the limit of advance.¹¹⁵ Instead of culminating, the swarm pushes out sentinel nodes (e.g., dismounted hunter-killer teams, acoustic sensors, and sleeper drones) along the likely avenues of approach for enemy reserves in order to support ambushes. This effectively establishes a screen that transitions into a lethal ambush when the enemy attempts to reinforce its position or forces.¹¹⁶ By interdicting the counterattack forces in their assembly areas or while they are on the move, the swarm denies the enemy the ability to regain the initiative, thereby securing the gains of the first two pulses.

The “pulse” of a swarm, therefore, is not a single volley from a single line of departure. Rather, it reflects a synchronized sequence generated from distributed launch sites that complicates enemy scouting and keeps the kill web intact when any one node is jammed, struck, or forced to move. From these dispersed positions, commanders employ staggered salvos timed to create tight time-on-target windows, so that decoys, jammers, loitering munitions, and follow-on fires arrive as a coordinated stack that overwhelms the enemy’s ability to recover between impacts. Dynamic targeting then takes over, as probes expose emitters, command posts, bridges, or reinforcement columns, and the swarm redirects payloads against the most valuable node in the moment rather than the one briefed the night before.

None of this works without an assessment loop. Each pulse must generate fresh battle damage indicators, update target priorities, and determine whether the next salvo should exploit, shift axes, or pause before the force burns through its own tempo. That feedback loop determines the next pulse.

PULSING IN KURSK

The initial sense-and-pull pulse in Kursk was a carefully synchronized infiltration. Two days prior to the heavy-armor crossing, small teams from the Ukrainian 80th Air Assault Brigade, enabled by SOF, infiltrated the border zone to map gaps and physically degrade defenses, effectively executing the doctrinal “reconnaissance pull” to guide the main force through the path of least resistance.¹¹⁷ Reuters reporting described Ukrainian units moving under heavy drone support and artillery fires, with additional special elements pushing even deeper with sabotage-style activity, all of which is consistent with shaping logic that blends reconnaissance, disruption, and rapid multi-axial movement to overload local defense responses.¹¹⁸

Simultaneously, Ukrainian EW units conducted signal surveys (i.e., identifying how the enemy communicates to support targeting) to facilitate jamming Russian communication networks and blinding their ISR drones. Denying key portions of the EM spectrum blinded Russian forces long enough for Ukrainian engineers to breach minefields and fortifications in relative secrecy, thereby ensuring that the physical corridors for the swarm were open before the first tank fired.¹¹⁹

Once the initial breach was achieved, the main (second) pulse demonstrated the swarming characteristic of simultaneity, where distributed mobile groups converged on key nodes rather than fighting a linear battle for every meter of ground. Instead of a monolithic column, Ukrainian forces advanced on multiple axes, utilizing FPV drones and precision fires to isolate Russian strongpoints such as the Sudzha border crossing while mobile armor bypassed those strongpoints to strike

deeper into the rear operational area.¹²⁰ These actions created the “dilemma of simultaneity” for the Russian command—reports indicate that Ukrainian units appeared “everywhere and nowhere,” paralyzing local decisionmaking as they struck logistics hubs and command posts well behind the perceived front line.¹²¹ The integration of loitering munitions provided the dispersed Ukrainian units with organic, precision artillery-like effects, allowing them to maintain the high tempo required to disintegrate Russian defensive integrity before reserves could mobilize.¹²² A U.S. Army analysis of Kursk stressed the importance of reconnaissance synchronization, compartmentalized planning, and concealment to deny indicators, as well as preparatory actions (including nonlethal effects) intended to degrade ISR and reinforce deception.¹²³

What is often missed in portrayals of the Kursk offensive is the integration of information warfare and the combination of effects across the physical, informational, and human dimensions. The operation was preceded by an increase in documented Ukrainian cyber activity in June and July 2024 that included attacks on public transportation networks as well as mobile and internet service providers.¹²⁴ In addition, Ukraine was actively running an information operation targeting Russian morale through the “I Want to Live” surrender hotline, which effectively attacked the cohesion of Russian conscript units by pushing targeted messages to their phones.¹²⁵

The third pulse of the Kursk offensive demonstrated the operational anticipation required to secure swarming gains, specifically by transitioning to a mobile defense that interdicted the inevitable Russian counterattack before it could reach contact. Recognizing that Russian doctrine relies on rapid reinforcement via rail and road, Ukrainian planners projected a screen of “sentinel” nodes—including deep-penetrating reconnaissance drones and SOF elements—along key routes.¹²⁶ This foresight enabled the “fires ambush” of a Russian reinforcement column near Oktyabrskoye, where HIMARS strikes destroyed a battalion-sized convoy of Russian trucks carrying infantry and ammunition while they were still on the march, miles from the engagement area.¹²⁷ Furthermore, distributed “hunter-killer” teams systematically targeted fuel tankers and pontoon-bridging equipment used to cross rivers, denying the Russian counterattack force the logistical energy required to sustain a coherent response and forcing them into a reactive posture.¹²⁸

Consolidate and Transition

The third phase of swarming focuses on consolidating gains to prevent culmination and reset the force for the next attack. After swarming, the force must reload, protect itself, and decide whether to attack again or, instead, shift to defense. In swarming terms, this requires a critical assessment of positioning relative to the next objective: The commander must determine whether the swarm can generate its next pulse from existing locations or if it must displace forward to extend its operational reach.¹²⁹ This decision ultimately dictates the transition of battlespace management—the previous “attack zone” transforms into a new “support zone,” necessitating a forward shift of the fire support coordination line to open up new deep areas for engagement.¹³⁰ This transition is a period of distinct vulnerability. As the swarm “reloads”—refitting drones, rearming precision fires, and processing new targeting data—it requires a dedicated security screen. Additional forces or a

“secondary swarm” must effectively shield the recovering main body from counterattacks, ensuring that the logistics tail can catch up to the teeth of the offensive before the next pulse is unleashed.

With either a new support zone established or the force refitted, the swarming operation transitions to a follow-on pulse attack, typically taking the form of an exploitation or pursuit.¹³¹ The decision to move forward transforms consolidation into a springboard. A “secondary swarm,” often acting as an advanced guard, pushes ahead of the main body to maintain contact with the retreating enemy and prevent the enemy from reorganizing or establishing a coherent defense. By attacking an enemy’s ability to retrograde and consolidate (e.g., through disrupting or destroying pontoon bridges, command vehicles, and rallying points), this forward element converts the enemy’s withdrawal into a rout.¹³² This allows the main force to launch a subsequent pulse against a disorganized opponent, effectively turning the initial tactical success into a wider operational victory.

Transition criteria should be explicit because the problem is whether the force can keep generating pulses faster than the defender can recover. As a planning factor, transition should begin either when the adversary restores more than roughly 60 percent of its pre-strike sensor picture over the main axis, or when the adversary can reestablish continuous target quality on friendly launch corridors for one full pulse cycle. At that point, the swarm is no longer operating inside a meaningful defensive gap. It is operating inside a recovering kill web.

Friendly criteria should be equally clear. As a planning factor, attrition among critical ISR, EW, and relay nodes should remain below 20 percent, while strike package attrition should remain below roughly 25 percent. Beyond those points, the force begins to lose the density required to recreate local overmatch at penetration.

Operational reach then becomes the final check. If distributed launch sites cannot rearm, recharge, and reposition enough systems to generate at least 80 percent of the next planned pulse before the enemy reconstitutes, the force should transition, even if the last attack produced local success.

CONSOLIDATING AND TRANSITIONING IN KURSK

In the Kursk campaign, the consolidation around the town of Sudzha illustrates the shift from “attack zone” to “support zone.” Once the Ukrainian 80th and 82nd Brigades seized the town, it was not treated merely as a conquest but instead immediately converted into a forward logistics and command hub to support the next operational push.¹³³ Reporting suggests that Ukrainian artillery and drone teams rapidly assessed their effective ranges and moved forward into this newly secured pocket, effectively shifting their fire support coordination lines deeper into Russia to range targets such as bridges.¹³⁴ Crucially, Ukrainian forces established a robust defensive perimeter around Sudzha, using FPV drones to protect the high-value EW and HIMARS assets refitting within the zone from Russian sabotage groups, thereby securing the “hive” as it prepared for the next pulse.¹³⁵

The campaign's shift toward the Seym River crossings illustrates the transition to pursuit. As the main body consolidated in Sudzha, forward elements pushed north and west to isolate the Glushkovsky district.¹³⁶ The systematic destruction of permanent bridges and the subsequent hunting of Russian pontoon engineering units by FPV drones acted as a "pursuit by fire," cutting off the escape routes for Russian units south of the river.¹³⁷ This action trapped Russian forces in a cauldron, preventing them from stabilizing a new defensive line while also setting the conditions for the next phase of the Ukrainian offensive.

Swarming Against the Integrated Air Defense

Future military campaigns will likely rely on the integration of semi-autonomous swarms to penetrate and dismantle layered enemy defenses. Modern IAMDs pose significant risks to high-value manned platforms such as fighter jets and form a critical layer of A2/AD bastion complexes. Breaking these defensive complexes requires employing networked masses of low-cost unmanned systems to saturate sensor grids, deplete interceptor magazines, and identify vulnerabilities within the defensive complex. These swarms serve as a vanguard, breaking the cohesion of the enemy network and thereby allowing exploitation by follow-on forces.

The use of swarming formations to defeat IAMD systems is a cost-effective method of setting conditions for launching deep strikes to support operational maneuver. Enemy radars, missiles, and command and control have to be blinded, disrupted, or destroyed to provide safe maneuver for aircraft to conduct deep strikes. SEAD is defined in joint doctrine as any activity that neutralizes, destroys, or temporarily degrades surface-based air defenses to create the necessary freedom of action for friendly air operations.¹³⁸ Rather than serving as a standalone mission, SEAD is a supporting function of offensive counterair designed to fracture an adversary's integrated air defense system (IADS) through two primary approaches: destructive means, which seek permanent system removal, and disruptive means, which employ jamming or deception to create a temporary window of safety.¹³⁹ SEAD is planned sequentially (preemptive shaping) or concurrently (simultaneous support), depending on the tempo of the campaign. Ultimately, successful SEAD requires the integration of joint capabilities and precise intelligence coordination to ensure that whether the suppression is theater-wide or localized, it effectively protects friendly forces against the chaos of contested airspace.¹⁴⁰

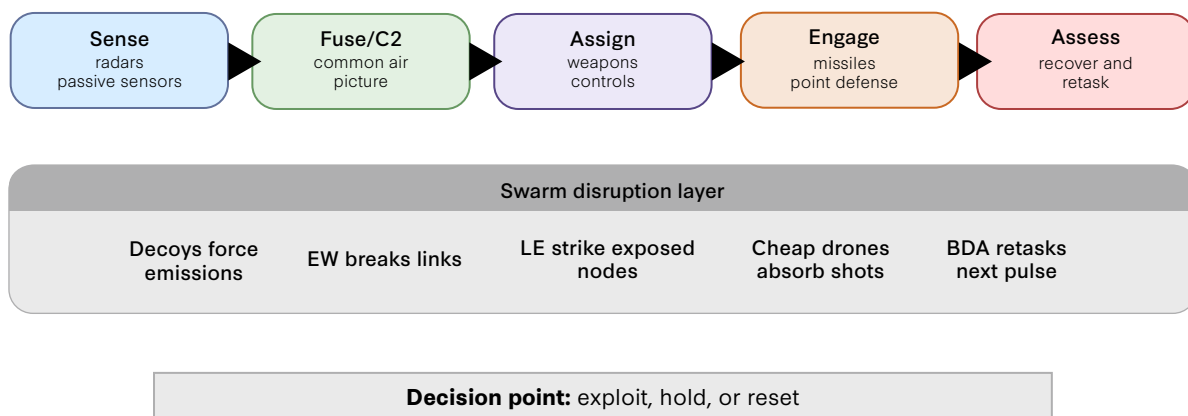
Denying enemy aircraft access depends on a labyrinth of sensors, jammers, and missile batteries as well as combat air patrols all connected as a layered defense in depth. This IAMD complex is both old and new. The idea of using battle-networked sensors as a modern bastion fort has endured since World War II. During the Battle of Britain, for example, a mix of radar stations and observers helped vector Royal Air Force Spitfires to intercept German bombers using the Chain Home system.¹⁴¹ This concept then evolved via the Semi-Automatic Ground Environment program in the early Cold War, which connected radars to computers to optimize jet and long-range surface-to-air missile intercepts of Soviet bombers.¹⁴²

In its modern form, the air defense bastion extends the battle network to create a mix of active and passive defense layers. Active networks such as the NATO Integrated Air and Missile Defence System mix medium- and long-range systems (e.g., SAMP/T, Patriots) with short-range air defenses and combat air patrols.¹⁴³ These active measures serve alongside passive defenses such as decoys, camouflage, installation hardening, and emissions control. The networks also integrate sensors, such as cell phones used as acoustic sensors in Ukraine and emerging C-UAS efforts such as the “European Drone Wall” and Joint Interagency Task Force 401.¹⁴⁴

Legacy approaches to SEAD face three critical failure points. First, the enemy is adaptable and can adjust radar profiles to obscure targeting while disaggregating and moving launchers to increase survivability. Second, a cost asymmetry exists where low-cost decoys attract million-dollar missiles, leading plans to over-emphasize one-off pulse attacks that create a temporary window at the expense of joint formations. Finally, modern approaches rely on brittle C2 architecture utilizing satellite constellations or airborne relays. These links are vulnerable, leading to overly centralized C2 of large missile salvos that struggle to overcome point defenses once identified.

As a result, legacy approaches relying on expensive manned aircraft and expensive, specialized munitions are increasingly vulnerable. Moreover, the high cost and limited numbers of these platforms make them risky propositions, while their reliance on centralized C2 leaves them open to disruption.

Figure 18: Swarm Versus IAMD Kill Chain



Source: CSIS Futures Lab.

A new operational paradigm must embrace the principles of mass and maneuver while disaggregating the strike pulse into a cosine wave.¹⁴⁵ This approach resembles a thousand arrows fired from mounted archers continuously on the move. The swarm creates repeated and overlapping pulses from many directions using a heterogeneous mass of unmanned systems carrying sensors, jammers, and high-explosive payloads. As illustrated in Figure 18, the swarm disruption layer systematically dismantles the IADS kill chain. Decoys deliberately force radar emissions to uncover concealed positions. EW platforms then break the critical communication links required to fuse a common air picture. As the defender assigns weapons to counter the incoming wave, loitering munitions strike those newly exposed command nodes. During the physical engagement phase, waves of cheap drones absorb expensive interceptor shots to deplete local magazines.

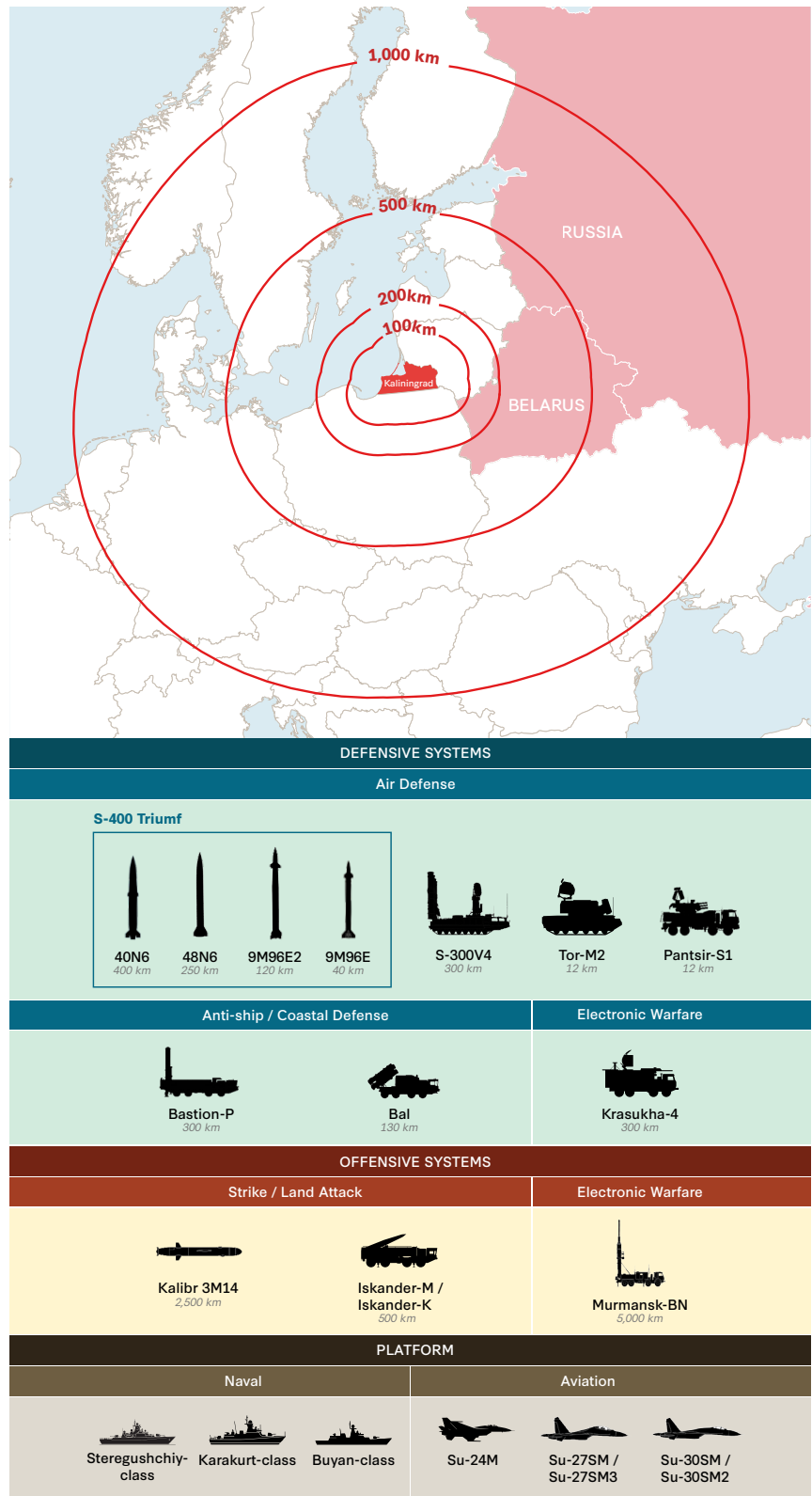
This networked coordination adds resilience and adaptability. Individual drones can sacrifice themselves without breaking the overall mesh network. The sheer mass saturates the airspace and degrades the defense's capacity to track targets, creating blind spots. The swarm further aids target deconfliction by routing trailing payloads away from high-risk areas. This dynamic routing is central to gaining an advantage. Prior planning often cannot account for the sheer complexity of an air defense network in contact and enemy adaptation. A swarming force operates as an adaptive system driven by continuous feedback loops where intelligence updates and battle damage assessment immediately retask the next pulse. The introduction of the swarm erodes the defensive bastion and creates opportunities to exploit emergent vulnerabilities.

Case Study: Kaliningrad

As adversaries mature their A2/AD capabilities, the density and lethality of modern IAMD pose unacceptable risks to high-value manned platforms. Regaining the advantage requires employing networked masses of low-cost unmanned systems operating in the air littorals to saturate sensor grids, deplete interceptor magazines, and identify vulnerabilities within the defensive complex.¹⁴⁶ In this manner, swarms can serve as a vanguard force that identifies and exploits gaps in support of follow-on forces.

Nowhere is this challenge more acute than in the Russian oblast of Kaliningrad. Situated between Poland and Lithuania, the Russian exclave functions as a strategic “bastion” designed to project power and deny NATO freedom of maneuver in the Baltic Sea region. The threat radiating from Kaliningrad is not merely a collection of ground-based batteries but rather a highly networked, multidomain IADS complex that integrates surface, subsurface, and aerial layers to sever NATO's access to the Baltic states.

Figure 19: Kaliningrad IAMD Capabilities



Source: CSIS Futures Lab.¹⁴⁷

The foundation of the Kaliningrad A2/AD complex is the ground-based sensor and shooter network. Russia has deployed multiple S-400 Triumf (NATO: SA-21 Growler) battalions to Kaliningrad, creating overlapping kill webs.¹⁴⁸ These systems utilize the 92N6E “Gravestone” fire-control radar and the 91N6E “Big Bird” acquisition radar to track targets up to 600 km away.¹⁴⁹ Armed with the 40N6E missile, the Triumf batteries can engage high-value assets (e.g., Airborne Warning and Control System [AWACS] and aerial-refueling tankers) up to 400 km away, effectively pushing NATO’s support assets well back into Polish airspace. This long-range layer is protected by medium-range 9M96E and 9M96E2 interceptors that can be launched from the S-400, as well as short-range Pantsir-S1 (NATO: SA-22 Greyhound) and Tor-M2 (NATO: SA-15 Gauntlet) systems, which provide point defense against precision-guided munitions and low-flying cruise missiles.¹⁵⁰

Russia’s Baltic Fleet, headquartered in Baltiysk, acts as a mobile extension of Kaliningrad’s IADS network. Modern surface combatants, such as the Steregushchiy-class corvettes, are equipped with the Redut vertical launch system, which fires 9M96 series missiles—the same interceptors used by the S-400 and S-350 ground systems.¹⁵¹ Furthermore, Russia’s newer Karakurt-class corvettes feature naval variants of the Pantsir-M system, providing robust point defense.¹⁵² These ships can data link with ground-based batteries, creating a mobile sensor-shooter network that complicates NATO targeting cycles by constantly shifting the geometry of the threat environment.

Perhaps the most potent kinetic threat comes from Russia’s 132nd Mixed Aviation Division based at the Chkalovsk and Chernyakhovsk airfields.¹⁵³ These bases host Su-27, upgraded Su-27SM3, Su-30SM, and Su-30SM2 fighters, the last of which is increasingly armed with the R-37M (NATO: AA-13 Axehead) air-to-air missile.¹⁵⁴ With a reported range exceeding 300 km and hypersonic terminal velocity, the R-37M is specifically designed to hunt “force multipliers” such as E-3 Sentry AWACS and KC-135 tankers, increasing the density of the A2/AD bubble and allowing Russian fighters to engage NATO aircraft while remaining under the protective umbrella of their own S-400s.

Russia also employs a sophisticated EW capability. The 841st Separate Electronic Warfare Center operates the Murmansk-BN, a strategic heavy jamming complex reportedly capable of disrupting high-frequency communications at ranges up to 5,000 km, potentially severing links between NATO headquarters and forward-deployed units.¹⁵⁵ This is complemented by the mobile Krasukha-4 EW system, designed to blind airborne radars and GPS-guided munitions.¹⁵⁶ These sensors and effectors are integrated through automated C2 systems such as the Polyana-D4M1, which fuses data from ground, sea, and air assets to provide a common operating picture and optimize target allocation across the IADS.¹⁵⁷

A potential strategy for NATO’s successful deployment of an operationalized swarm against the Kaliningrad A2/AD complex would include the following steps:

SET CONDITIONS

To reduce losses, NATO first would need to disrupt the IAMD kill chain. Decoys and emitters would force Russian sensors to reveal themselves. To do so, NATO would first have to set the conditions through aggressive sensing and preparation. Before the first kinetic strike, NATO would conduct “signal surveys” using high-altitude assets and clandestine sensors to map the EM “pattern of

life” of the Kaliningrad IADS, data critical for programming the autonomous logic of the swarm to recognize and prioritize specific emitters, such as the 92N6E “Gravestone” fire-control radar.¹⁵⁸ Simultaneously, NATO planners would execute force closure by prepositioning containerized swarm systems—disguised as commercial freight—into staging areas in Poland and Lithuania. This shell game would complicate Russian targeting while ensuring that the subsequent swarm can be generated from dispersed locations rather than vulnerable air bases. To further degrade Russian situational awareness, NATO would deploy low-cost decoys and emitters along the border to mimic high-value assets, effectively weaponizing the signal-to-noise ratio and compelling Russian operators to radiate their sensors, thereby revealing their positions.

PULSE

Once conditions are set, the operation transitions to the pulse phase, a rhythmic application of mass designed to overwhelm the adversary’s decisionmaking cycle. The initial pulse functions as a sense-and-pull maneuver, where semi-autonomous launched effects and loitering munitions infiltrate the air littorals to probe the periphery of Russian defenses. Instead of a blind assault, these assets trigger the IAMD network, forcing Russian batteries to light up their engagement radars, providing swarm targets. When a node detects an active emitter, it validates the target and “pulls” the main body of the swarm toward the gap. This triggers the main pulse, a concentrated convergence of lethal drones arriving simultaneously from multiple vectors (i.e., ground-launched swarms from the Suwalki corridor, sea-launched swarms from the Baltic, and air-launched effects from standoff aircraft). This saturation attack overwhelms the fire-control channels of the Russian S-400 and Pantsir systems, depleting their magazines against lower-cost drones while high-explosive payloads strike critical radar and command nodes.

Last, anticipating a Russian counterstrike, the swarm executes a final pulse by transitioning to a mobile defense. “Sentinel” nodes consisting of multiple drones loiter over likely reload sites and airfields, creating an immediate “fires ambush” for Iskander transporter erector launchers or aircraft attempting to sortie. The goal is not to destroy every weapon, but rather to break the chain that lets sensors find targets and weapons engage them.

The pulse depends on rapid battle damage assessment loops. Command teams fuse physical and functional swarm indicators such as radio frequency shifts, telemetry, optical feeds, and other signatures to assess defensive behavior under stress. The key to this data collection is determining whether the Russian IAMD network can still find, assign, and engage targets at scale. When it cannot, follow-on forces can launch attacks against high-value targets. In SEAD terms, the objective is temporary sanctuary rather than total destruction. The force needs enough functional suppression of sensors, command nodes, and weapons-control loops to open a usable window for the next echelon before the enemy reconstitutes.

CONSOLIDATE AND TRANSITION

The NATO swarming operation concludes with consolidation and transition. Commanders assess the integrity of the breach, and if the IAMD threat is neutralized, the “attack zone” transforms into a “support zone,” allowing the fire support coordination line to shift deeper into Kaliningrad. This opens the airspace for manned aircraft to conduct heavier strikes and interdiction with reduced

risk. To prevent the Russian IAMD network from reconstituting, a secondary swarm is launched as a pursuit force. Recognizing that Russian doctrine emphasizes mobility for survivability, this advanced guard would hunt disaggregated elements of the air defense network hiding in urban or forested terrain, securing the air corridor for the broader joint campaign. Transition criteria in the Kaliningrad vignette would be established before launch and linked to determining whether the swarm has opened a true corridor, a temporary seam, or a gap that is already closing.

During this phase, logisticians will race to push additional resources forward to swarm launch points, ensuring additional capacity is in place to mitigate risks and seize opportunities that emerge during the transition. These resupply systems should be integrated with predictive analytics that extend back to rear areas and global supply chains to ensure a constant flow of information produces a continuous flow of multiple classes of supply.

Conclusion

The Kaliningrad vignette illustrates how the operational framework can restore freedom of action against a mature integrated air and missile defense network. NATO first sets conditions by mapping the EM pattern of life, prepositioning containerized launch nodes in Poland and Lithuania, and using decoys to force Russian sensors to radiate. The force then delivers repeated pulses. Low-cost launched effects probe the air littoral, pull lethal payloads toward exposed emitters, saturate fire-control channels, and attack the command links that hold the defensive complex together. Assessment focuses on whether the Russian network can still find, assign, and engage targets at scale. When it cannot, NATO consolidates and transitions by converting the temporary opening into a support zone for manned aircraft and long-range fires. A secondary swarm then hunts mobile air defense elements and protects the corridor from reconstitution. The objective is functional suppression that lasts long enough for the next echelon to act before the Russian network recovers.

Executing this concept requires defense reforms that emphasize interoperability, sustainment, and adaptation. NATO needs dispersed storage and launch sites, coalition-releasable mission data, and reliable battle-damage assessment under contested conditions. It also needs a common battle network that allows sensors, decoys, jammers, and strike payloads to operate as one. Dedicated units must be trained to generate successive pulses, repair and rearm systems forward, and apply explicit criteria for exploiting, holding, or resetting the corridor. These requirements point toward a multi-vendor family of launched effects supported by open architecture, rapid software updates, prepositioned stocks, and recurring joint exercises. Those exercises should measure corridor survivability, sensor suppression, command coherence, and the time required to regenerate the next pulse. A first salvo may disrupt Kaliningrad's IAMD complex. The larger operational system turns that disruption into the tempo required for a broader joint campaign.

Swarming Against Integrated Sea Control

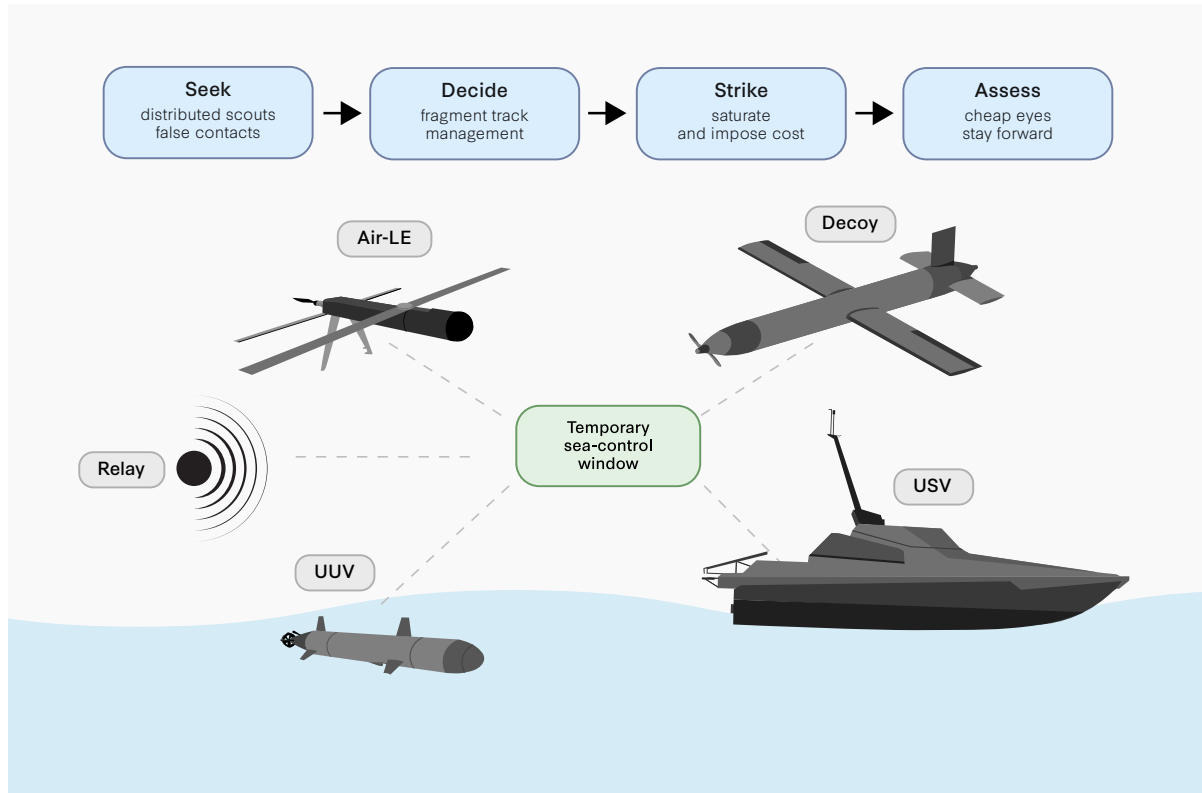
Modern sea control is no longer a contest fought only by ships exchanging salvos over the horizon. It is a duel between targeting complexes as rival forces seek to find, strike, and assess faster and more accurately than an opponent across multiple domains. Consistent with Wayne Hughes's conceptualization of sea power, maritime advantage begins with the ability to find the enemy, preserve one's own scouting, disrupt the adversary's command and control, and convert information advantage into effective long-range fires from the seabed to space. Sea control, therefore, is the temporary ability to generate multidomain effects sufficient to use a specified maritime space for one's own purposes while denying that same freedom to the enemy.¹⁵⁹

Sea control operations are those operations designed to secure use of the maritime domain by one's own forces and to prevent its use by the enemy. – JP 3-32

As depicted in Figure 20 below, this framework also clarifies where drone swarms create advantage. They intervene at multiple stages. First, swarms play a role in Hughes's seek function by expanding sensing and complicating the adversary's picture with decoys, false contacts, and distributed collectors. Second, in the decide function, they intervene by attacking the enemy's command architecture, forcing emissions, fragmenting track management, and slowing the targeting cycle. Third, swarms support strike capabilities by creating saturation, cost imposition, and attrition

across the kill web rather than only at the point of impact. Finally, they intervene in the assessment function by keeping cheap eyes and passive collectors forward after the first exchange, allowing the larger fleet to determine whether the adversary's network is broken, displaced, or simply disrupted.

Figure 20: Swarms in the Sea-Control Cycle



Source: CSIS Futures Lab.

Seen through Hughes's logic of salvo competition, the critical shift that swarms facilitate is from a single decisive missile exchange to repeated windows of convergence across multiple domains and dimensions. The desired operational dilemma departs from massing one overwhelming salvo that breaks the enemy system (i.e., destruction). Rather, the objective is to generate successive pulses that repeatedly blind, bait, strike, and assess before the enemy can fully reconstitute. Pulse, in other words, is salvo competition adapted to the age of battle networks. It is a rhythm of distributed scouting, synchronized fires, and rapid reassessment that creates temporary local sea control without incurring the costs of enduring maritime supremacy.

Seen in this light, understanding the challenge of disrupting integrated sea control in the South China Sea requires first defining the doctrinal objective. Both U.S. Joint Publication 3-32 (*Command and Control for Joint Maritime Operations*) and NATO Allied Joint Publication 3.1 (*Allied Joint Doctrine for Maritime Operations*) define sea control as the condition in which a military force has the freedom of action to use the maritime domain for its own purposes in specified areas and for specified periods of time while simultaneously denying or limiting similar use to the enemy.¹⁶⁰ In NATO

doctrine, sea control is a subset of approaches to achieving maritime superiority that also includes forcible entry, maritime raids, commerce warfare, and other shaping activities that set conditions for concentrating forces in and through the maritime domain. In U.S. joint doctrine, sea control is one of five core capabilities, alongside forward presence, deterrence, maritime power projection, and maritime security. According to Naval Doctrine Publication 1 (NDP 1) sea control is the central mission of the U.S. Navy.¹⁶¹ Increasingly, sea control requires multidomain effects, including space-based communication and targeting, EM spectrum and cyber operations, and air- and land-based missiles and sensors.

Sea control remains an enduring feature of long-term competition and conflict. From the ancient triremes of Salamis to the modern aircraft carrier strike groups, the struggle for control of the seas has been a defining feature of warfare throughout history that adapts based on new ideas and technology across the ages. The Battle of Salamis, where a smaller Greek fleet decisively defeated the Persian navy, set in motion strategic thinking about the utility, if not necessity, of adapting sea power.¹⁶² The combination of using terrain and taking advantage of key differences in the correlation of forces (i.e., heavier Athenian ships) to identify asymmetries to exploit remains a core feature of sea control concepts. As distances increased—for example, from regional to global sea lines of communication (SLOCs) and supporting basing infrastructure—theorists developed new approaches ranging from decisively defeating the enemy’s fleet in Mahan’s naval rendering of Jominian lines to waging a series of distributed blockades and smaller battles that complicated the ability of the enemy to mass in Sir Julian Corbett’s rejoinder.¹⁶³ The emergence of cheaper ways to sink a ship added new approaches to interdiction, denial, and commerce raiding in the *Jeune École* as a way of denying sea control to larger powers.¹⁶⁴

Terrain and technology continue to define the struggle for sea control. No longer restricted to the oceans, longer-range strike weapons launched from multiple domains have meant that control of the sea increasingly involves control of the air and access to space. More specifically, airfields, radar installations, and missile batteries hundreds of miles inland present an exponential challenge to the extent the network is integrated. The maritime littoral becomes interior lines, enabling adversaries to create new attack vectors faster than defenders can respond, driving the need to conduct standoff strikes and invest in more defensive capabilities. Therefore, the modern fleet, led by a carrier strike group, has to maintain an early warning network, sustain defensive configurations, and use aircraft and long-range missiles to wage battles well beyond the line of sight. As a result, integrated sea control is prone to extremes in the offense and defense—distributed fleets conduct massed standoff strikes against limited objectives in an effort to overwhelm the defense and deny the ability of the target to return the favor. This process is best captured in Wayne Hughes’s mantra “fire effectively first” and the U.S. Navy concept of Distributed Maritime Operations.¹⁶⁵

Put simply, new technologies, such as hypersonic missiles and unmanned systems, have created new challenges and new opportunities for naval forces simultaneously. The proliferation of A2/AD capabilities has made it more difficult for traditional naval powers to operate freely in certain regions. Asserting sea control becomes highly complex due to a robust combination of threats. Threats include a mix of modern surface combatants equipped with sophisticated anti-ship

weaponry, stealthier submarines, continuous air patrols for reconnaissance and strike, satellite constellations, and long-range missile systems, to name a few. Together, these systems create a whole greater than its parts, as the elements complement one another, orchestrating to lock down key maritime SLOCs and prevent the movement of adversarial forces. The traditional form of achieving sea control Mahan described with large fleets fighting a decisive battle—outside of Midway-like pulse attacks—becomes less likely with each new technology or strategy.

Furthermore, legacy approaches, including conventional naval warfare strategies, often face limitations when countering this complex mesh of threats. Traditional defensive methods primarily employ large capital surface ships and manned submarines, presenting considerable risk in light of advanced enemy assets and technologies. These costly assets notably lack the flexibility to simultaneously handle all facets of the threat and, moreover, often fall short in maintaining the pace of warfare due to operational and logistical constraints. Additionally, the inherent risks involved in operations with large, manned fleets increase the risk of mass casualties, which adversaries may use for propaganda gain.

Establishing localized, multidomain sea control over the South China Sea is a core strategic imperative tied to regime security, economic survival, and regional hegemony for the PRC. The PRC seeks to dominate this waterway not only to secure the vital SLOCs that underwrite its own economy but also to create a highly protected, deep-water “bastion” for its fleet of Type 094 (Jin-class) nuclear-armed ballistic missile submarines operating out of Yulin Naval Base on Hainan Island.¹⁶⁶ Furthermore, achieving sea control in this region establishes a dense A2/AD buffer zone—often termed “counterintervention” in PLA doctrine—designed explicitly to deter, delay, or defeat U.S. and allied power projection within the first island chain during a regional crisis such as a Taiwan contingency.¹⁶⁷

To accomplish this, the PLA has operationalized the multidomain character of modern maritime dominance, heavily relying on a core doctrine based on paralyzing enemy battle networks rather than merely annihilating enemy forces.¹⁶⁸ Far from relying solely on a surface fleet, the PLA’s sea control architecture integrates a pervasive command, control, communications, computers, combat systems, intelligence, surveillance, reconnaissance, and targeting (C5ISR-T) grid that fuses targeting data from space-based Yaogan surveillance satellites, land-based over-the-horizon sky-wave radars, and seabed acoustic arrays often referred to as the “Underwater Great Wall.”¹⁶⁹ This multidomain scouting network is seamlessly tethered to a decentralized array of cross-domain “shooters,” ranging from H-6K bombers and stealthy attack submarines to land-based DF-21D and DF-26 “carrier-killer” anti-ship ballistic missiles fielded by the PLA Rocket Force hundreds of miles inland.¹⁷⁰

This kill web is physically anchored by militarized artificial islands in the Spratly and Paracel archipelagos, where outposts such as Fiery Cross, Subi, and Mischief Reefs function as stationary joint force bases projecting overlapping umbrellas of EW, surface-to-air missiles, and anti-ship cruise missiles.¹⁷¹ By shielding this physical network with aggressive cyber and EM spectrum operations designed to paralyze an adversary’s C2, the PLA has transformed the South China Sea into a fortified multidomain bastion, further illustrating that modern sea control is no longer a

localized naval clash but instead requires dominating sensor-to-shooter kill webs across land, sea, air, space, and the EM spectrum.

Figure 21: Fiery Cross Reef: Rock Located in the Spratly Islands and Occupied by China Since 1988



Source: CSIS Asia Maritime Transparency Initiative/Vantor.

With these considerations in mind, a distributed swarm gives the force more scouts, decoys, and low-cost strike options across the surface, subsurface, and air domains. In the network-centric framework that has come to define modern sea control, an array of small, unmanned systems across the surface, undersea, and air domains collectively form a distributed, semi-autonomous swarm. Their capabilities range from ISR to striking high-value enemy assets, enabling the swarm to adapt promptly to emerging threats. These swarms can disrupt, degrade, or destroy enemy anti-ship missile systems, surface combatants, submarines, or air patrols, providing a more effective barrier against enemy maneuvers. Moreover, with the ability for swarms to operate autonomously and maintain coordination even under contested

conditions, they offer greater survivability while minimizing the risk of human casualties compared to legacy approaches.

Imagine a swarm of unmanned surface vessels, underwater drones, and aerial platforms, all working in concert to deny adversaries control of the seas. This heterogeneous swarm, with its diverse capabilities and decentralized architecture creates a new form of *Jeune École*, a nineteenth-century asymmetric theory of naval warfare.¹⁷² Small air and naval swarms overwhelm larger capital ships.

Even demonstrating the ability to use swarms to strike capital ships and other platforms used for integrated sea control threatens freedom of action. The possibility of capital ships being sunk by cheap drones increases the costs the adversary has to pay in time, resources, and risks to achieve sea control. Swarms offer forces the possibility of overwhelming enemy defenses through sheer numbers, saturating their sensors and degrading their ability to track and engage individual targets, thus complicating counterforce and C2 countermeasures (C2CM) in Hughes's framework for naval tactics. Unmanned surface vessels could harass enemy ships and submarines, while aerial drones could provide targeting data and conduct strikes against high-value assets, creating opportunities for scouting and anti-scouting as well as firepower strikes designed more to disrupt than defeat enemy fleets and their supporting land-, air-, and space-based networks. Finally, underwater drones could lay mines, disrupt communications, and even launch torpedo attacks, placing the adversary on the horns of a multidomain dilemma.

A swarm provides several unique advantages in a sea control conflict. First, the swarm's distributed nature would make it difficult for an adversary to neutralize and would create burdens on intelligence and decision support systems (e.g., C2CM) as enemy fleets hunt the proverbial needle in a haystack. Even if individual units within a swarm were destroyed, the overall network would remain intact, allowing it to continue its mission and forcing the enemy to expend valuable resources and potentially expose its own vulnerabilities. A swarm's flexibility would be another key advantage, in particular the fact that a swarm could be rapidly reconfigured to respond to changing threats and objectives. For example, if the enemy attempted to concentrate its forces, the swarm could disperse to avoid detection and then converge on the enemy's flanks and use the EM spectrum to degrade targeting and counterforce capabilities.

Consider a hypothetical U.S. and allied counter-sea control campaign in the South China Sea. Its objective is limited and operational rather than absolute (i.e., total victory). Specifically, the goal is to deny the PLA the ability to use a defined maritime box as a secure battlespace for maneuver, scouting, and strike support during a wider regional contingency. In this context, sea control does not mean permanent maritime supremacy, but rather temporary allied freedom of action to move naval, air, and support forces through a specified area while denying the PLA reliable targeting and maritime maneuver inside that same space. The desired end state is a window of hours to days in which Chinese island outposts, maritime militia screens, and fleet scouting networks cannot generate coherent targeting against allied maneuver, thereby allowing reinforcement, sustainment, and follow-on joint operations to proceed at acceptable risk.

In this scenario, which prioritizes fungibility as a design feature, U.S. planners ensure that regardless of a node's primary domain—air, sea, subsurface—each is comprised of shared modules capable of acting upon a range of mission parameters such that a node that originally focused on jamming enemy communications can be quickly, and easily, reconfigured to, for example, deliver strike capacity instead. Though this feature increases initial costs, it preserves the ability to rapidly reconfigure payloads and create different network effects. In effect, this fungibility creates a constantly shifting series of surfaces that alter opportunity costs for the adversary and increase the risk of a mistake (i.e., decision failure), thereby creating cascading effects (i.e., positive feedback loops) and new asymmetries to exploit. In other words, the shifting attack surfaces enabled by the fungibility described above put the swarming attackers in a position to exploit the property of emergence in complex systems.¹⁷³

Since the networked swarm can affect multiple parts of the integrated sea control system, enemy commanders must shift resources from firepower and maneuver to anti-scouting. As time passes and the swarm gets closer, the adversary experiences diminishing marginal returns that, along with counterforce measures, create friction. The inherent opportunity cost involved in defending against the small, disaggregated, and ambiguous swarm undermines integrated sea control, an effect similar to why there were so few major naval battles in World War I: a mix of mines, torpedoes, and new intelligence networks complicated the search for Trafalgar-style decisive fleet engagements. In fact, the modern swarm is more likely to “cross the T” than a large combatant in the modern character of maritime conflict.¹⁷⁴ Assuming the swarm can get into range or pull the enemy out of position, its ability to exploit attack surfaces increases faster than the enemy can respond. In other words, in what analysts call “the interceptor trap,” an adversary may be able to use a million-dollar interceptor to down a \$10,000 drone, but in doing so they fall into a resource trap unsustainable in any protracted conflict.¹⁷⁵ The swarm creates a significant cost problem for the defender, with defensive costs rapidly outpacing those of the offense (i.e., affordable mass). A defender may spend an expensive interceptor to destroy a single cheap drone; while effective in limited-number drone attacks, that exchange becomes hard to sustain over time or against swarms.

Returning to the current scenario, the U.S. planners can create a neo-Jeune École course of action built around the swarm. In order to counter the range advantage afforded to large fleets, working alongside their partners and allies, planners develop scaled systems that can fit in standard shipping and Quadcon containers, facilitating ease of transport for air, ground, and sea platforms as well as increasing deception potential. Planners also build in design specifications to enable rapid domain transition to extend their lines, including small cranes and other support systems that decrease the time it takes to move a “swarm in being” from a truck to an aircraft or to a ship. Like the SEAD package, this system has organic power generation, ease of maintenance, and training and planning capabilities. In fact, these transportation, maintenance, and training and planning capabilities should be open architecture and modular so that they can be easily integrated both with other naval strike assets the partner nation has and with U.S. programs such as Replicator.

Case Study: The South China Sea

To dismantle the PLA's integrated sea control and degrade its A2/AD bastion in the South China Sea, U.S. and allied forces are currently betting heavily on the Distributed Maritime Operations (DMO) doctrine. This concept, championed by the U.S. Navy, seeks to counter the PLA's dense sensor-shooter networks by spreading the lethality of the U.S. fleet across a wider geographic area. Under DMO, dispersed surface action groups, guided-missile submarines, and carrier strike groups aim to generate overwhelming "pulse attacks"—massive, synchronized salvos of exquisite, long-range, precision anti-ship missiles, such as Long-Range Anti-Ship Missiles and Maritime Strike Tomahawks, fired from beyond the range of Chinese defenses. The logic is to overwhelm the PLA's Aegis-like Type 055 destroyers and island-based air defenses in a single, decisive Mahanian strike, temporarily tearing a hole in the PRC's A2/AD bubble to allow allied forces freedom of maneuver.

However, this legacy pulse approach presents severe operational and strategic vulnerabilities. First, relying on large, expensive, and relatively scarce manned platforms to deliver these salvos plays directly into the teeth of China's land-based anti-ship ballistic missile kill webs, which are specifically designed to hunt such high-signature capital ships. Furthermore, generating a sufficient missile pulse to create a large enough A2/AD hole often requires the fleet to either concentrate geographically or to emit key signatures to coordinate the strike, exposing the very platforms DMO intends to protect. Most critically, exchanging multi-million-dollar interceptors to defend these ships against incoming salvos, or using exquisite strike weapons to target relatively low-value PLA outposts, creates an unsustainable cost-exchange ratio and a brittle logistical dependency.

A lower-cost swarming approach shifts the burden from a few large ships to many expendable nodes and is consistent with new ideas emerging as part of the Hedge Strategy.¹⁷⁶ Instead of relying on the vulnerable arithmetic of legacy pulse attacks, U.S. and allied forces employ a networked, neo-Jeune École swarming approach. This strategy leverages precision mass, extreme cost asymmetry, and cross-domain uncrewed systems to systematically dismantle the PLA's C5ISR-T grid from the inside out. By shifting the burden of attack from a few highly prized surface combatants to thousands of disposable, autonomous nodes, this swarming concept effectively blinds the PLA's "system of systems" and denies the PRC control of the maritime domain without risking the core of the U.S. fleet.

Figure 22: Chinese Bases in the South China Sea



Note: Group placements are possible positions in a potential conflict. They are not representative of actual PLAN and allied positioning.

Source: CSIS Futures Lab.

SET CONDITIONS

Setting the conditions to fracture the PLA's sea control requires a persistent, distributed effort to map the environment and preposition forces without triggering preemptive escalation. First, allied forces must aggressively sense and map the multidomain "pattern of life" within the South China Sea. Because the PLA relies on a fused scouting network—ranging from the seabed Underwater Great Wall to space-based Yaogan satellites and shore-based over-the-horizon radars alongside sensors concealed in maritime militia—allied planners deploy low-signature autonomous underwater vehicles, passive acoustic gliders, and cyber reconnaissance elements to conduct deep signal surveys. This mapping identifies the critical data links connecting the air, sea, and

space assets along militarized artificial islands (e.g., Fiery Cross, Subi, Mischief Reefs) to mainland command centers.¹⁷⁷

Simultaneously, planners execute OPE through a massive logistical shell game. Leveraging the concept of containerized, fungible payloads—aligned with the Pentagon’s Replicator initiative and studies on “inside-out” defense concepts designed to deny the PRC a fait accompli—teams distribute thousands of standard shipping containers and Quadcons containing unmanned surface vessels (USVs), loitering munitions, and aerial EW drones across the first island chain.¹⁷⁸ With these payloads hidden aboard contracted commercial shipping, allied coast guard vessels, and dispersed U.S. and allied vessels throughout the archipelagic geography of the Philippines, the resulting dormant motherships complicate PLA targeting. The sheer volume of potential launch vectors places an enduring strain on Chinese ISR, forcing PRC forces to track every container and vessel, thereby degrading their integrated sea control bandwidth before a single shot is fired.

With the network mapped and the swarm prepositioned, the operation transitions to the shaping phase, utilizing an initial, intermittent pulse designed to execute reconnaissance pull and weaponize the signal-to-noise ratio. Rather than a massed kinetic assault from distant destroyers, allied forces unleash a wave of low-cost, semi-autonomous USVs and aerial decoys from the dispersed motherships, probing the outer edges of the PLA’s defensive rings.

This distributed movement to contact deliberately stimulates the PLA’s battle networks. By mimicking the radar cross-sections and acoustic signatures of high-value U.S. assets, the swarm forces the PLA to radiate key radars on the Spratly Islands and vector its People’s Armed Forces Maritime Militia and China Coast Guard interceptors. With this action, the United States and its allies weaponize the adversary’s feedback loops. When an active PLA emitter or patrol vessel engages an expendable decoy, the swarm node instantly passes a target-quality track back to the broader mesh network. The swarm thus identifies the exact geometries of the PLA’s active kill webs, fixes the enemy with electronic fires, and pulls the lethal main body of the swarm toward the identified blind spots in the C5ISR-T grid.

PULSE

Once the gaps in the PLA’s scouting network are verified, the main swarming pulse strikes with overwhelming simultaneity across the surface, subsurface, and air domains. This phase applies Wayne Hughes’s famous naval maxim to “fire effectively first,” but distributes that fire across hundreds of semi-autonomous nodes rather than a single salvo.¹⁷⁹ The objective is to paralyze PRC C2 and targeting infrastructure, thus neutralizing the PLA’s ability to execute its system destruction warfare doctrine.¹⁸⁰

Beneath the waves’ surface, unmanned underwater vehicles (UUVs) sever or manipulate seabed acoustic arrays and lay smart mines outside harbor entrances of the militarized artificial islands, trapping any PLAN combatants in port and also denying them reload sites. On the surface, wolfpacks of autonomous USVs equipped with EW modules and kinetic payloads work alongside launched effects to swarm the dispersed PLA surface action groups. This forces advanced Chinese cruisers such as the Type 055 to exhaust their multi-million-dollar vertical launch system magazines

engaging cheap drones, creating a resource trap that leaves them defenseless against follow-on allied anti-ship missiles. Swarms of loitering munitions converge on the Spratly and Paracel Islands outposts. These aerial swarms avoid heavily fortified bunkers and instead crater runways, destroy exposed radars, and neutralize the communication arrays that link the South China Sea bastion to the mainland PLA Rocket Force.

Measures of effectiveness for the pulse attack should focus on the integrity of the enemy kill web rather than simply platform counts. The first indicator is reduced track quality, measured by the adversary's inability to sustain continuous custody of allied ships, expeditionary bases, or logistic nodes in the contested area. The second is forced emissions from key radars, data links, maritime patrol nodes, and relay systems that reveal the architecture of the network and confirm that the swarm is compressing the enemy's decision cycle. The third is the creation of recurring targeting gaps, meaning periods in which the PLA cannot fuse a recognized maritime picture across the corridor. The fourth is corridor denial, defined as the adversary's inability to cue anti-ship fires into at least one critical maneuver route with acceptable confidence. The fifth is recuperation time, or how quickly the adversary can restore emissions, rebuild track quality, and regenerate local sensor coverage after each pulse.

CONSOLIDATE AND TRANSITION

Having blinded the PLA's local scouting networks and depleted its interceptor magazines, the allied force must consolidate its gains to prevent the PRC from reconstituting sea control. The maritime space previously dominated by the PLA transitions into a temporary support zone. As the swarm "reloads" via forward-deployed logistical hubs—such as expeditionary advanced bases in the Philippines—a secondary swarm pushes forward to establish a mobile defensive screen.

This sentinel force of loitering USVs and acoustic-monitoring UUVs is deployed along critical maritime chokepoints and approaches from the PLA's Yulin Naval Base on Hainan Island. If the PRC attempts a naval counterattack to restore its A2/AD bubble, this advanced guard serves as a tripwire, permitting mobile fires to ambush and interdict reinforcements before they can reach the contested zones. Under the protective canopy of this blinded and chaotic environment, allied manned capital ships and submarines can finally maneuver into the South China Sea with acceptable risk, exploiting the fractured A2/AD network to execute the broader joint campaign and secure the SLOCs.

Figure 23: Chinese Missile Capabilities



Source: "China," *Missile Threat*, CSIS, updated March 18, 2026, <https://missilethreat.csis.org/country/china/>.

Crucially, the logic of this swarming campaign is intrinsically tied to escalation management, ensuring that the United States and its allies can achieve operational success beneath the nuclear threshold. Breaking the PLA's integrated sea control via legacy operational concepts historically required deep, kinetic strikes against the Chinese mainland to destroy over-the-horizon radars, command nodes, and PLA Rocket Force missile bases (e.g., DF-21D, DF-26, and DF-27 launchers).¹⁸¹ However, as extensively documented in previous studies, striking dual-use command nodes or mainland missile bases directly threatens the regime's strategic nuclear deterrent.¹⁸² Because China's conventional and nuclear C2 architectures are deeply entangled, kinetic strikes on the mainland run an extreme risk of being misinterpreted as a preemptive counterforce attack, highly incentivizing a nuclear response.

The swarming approach actively mitigates this risk by shifting the geometry of the attack and separating the "archer" from the "eyes." The swarm disrupts offshore sensors and scouts, as well as orbital ones, rather than attacking mainland launchers. Because the mainland launchers cannot hit what they cannot see, their lethality is neutralized without dropping a single bomb on the Chinese mainland. Therefore, by focusing the swarm's non-kinetic and kinetic effects entirely on offshore

nodes—specifically the PLAN fleet at sea, the maritime militia, and the isolated artificial islands in the South China Sea—allied forces render the mainland-based anti-ship ballistic missiles useless without ever crossing the geographical red line of the Chinese coast. The swarm sinks the pickets, blinds the island-based radars, and jams the satellite downlinks, effectively winning the C5ISR-T fight in the maritime and space domains. This approach allows the joint force to dismantle the PLA's integrated sea control and win the operational campaign while tightly managing escalation, successfully containing the conflict beneath the nuclear threshold.

Conclusion

The South China Sea vignette illustrates how the swarming operational framework can contest integrated sea control by attacking the scouting and targeting architecture that makes Chinese long-range fires effective. Allied forces set conditions by mapping the multidomain pattern of life, distributing containerized air, surface, and subsurface nodes across the first island chain, and using decoys to stimulate PLA sensors and maritime screens. In the main pulse, electronic warfare and uncrewed systems converge on the connective tissue of the PLA kill web. They disrupt data links, blind island radars, crater runways, harass patrol vessels, and draw down interceptor magazines. Continuous assessment determines whether the PLA can maintain target custody, fuse a recognized maritime picture, and cue anti-ship fires into critical corridors. It also measures forced emissions and recuperation time. Once a window opens, the force consolidates and transitions. A secondary swarm screens chokepoints and likely reinforcement routes while allied manned forces exploit temporary sea control. Success is a window lasting hours to days for reinforcement, sustainment, and follow-on joint operations.

This approach surfaces key requirements. The joint force needs a cross-domain family of fungible swarm systems that can move among commercial vessels, coast guard platforms, expeditionary bases, aircraft, and naval ships. Prepositioned launch and repair nodes must be paired with common components, assured navigation, coalition-releasable data, and mesh networks that continue operating when satellite or terrestrial links degrade. Software and payloads must adapt quickly as the PLA changes signatures and tactics. Commanders also need escalation-control rules that focus attacks on offshore sensors, scouts, and artificial-island infrastructure. This geometry reduces pressure for strikes on mainland command and missile sites. These requirements also point toward distributed sustainment, an airborne relay layer, and recurring exercises that test whether the force can generate a second pulse before the PLA restores its C5ISR-T grid.

Swarming Against a Defense in Depth

The defense has always been the stronger form of war.¹⁸³ This is especially true in situations where the defense is able to tie into terrain, array in multiple, successive fortified lines, and integrate intelligence, obstacles, and fires across the depth of the battlefield. The deeper the attacker advances, the higher the attritional toll.

Defense in depth is when a commander has enough space to force the attacker into a series of successive engagements against dug-in forces. Rather than wagering success on a single forward line, the defender arrays mutually supporting positions, obstacles, reserves, and planned fires in successive belts so that the attacker must breach, reorganize, and breach again. The trade-off is sacrificing space to slow the enemy and change the correlation of forces. Depth in this form gives the defender more opportunities to identify the main effort, concentrate fires, shift reserves, and counterattack while also preventing a single local penetration collapsing the entire position.¹⁸⁴

The Italian-German Gothic Line in northern Italy during World War II illustrates this defensive strategy. Anchored on the north Apennines, the German defense used mountainous terrain, fortified positions, and successive defensive belts to slow the Allied advance toward Bologna and the Po Valley. As outlined above, this defense in depth did not need to be impenetrable to be operationally useful—it only needed to delay the attacker, increase attrition, and buy time for the defender to reposition and counter. The Gothic Line did just that from the initial Allied attack (Operation Olive, August 1944) until March 1945 (i.e., Operation Encore), when the line was breached, allowing the final Allied campaign in Italy. The logic of defense in depth applies in 2026, though outer belts are reinforced by drones, sensors, and EW rather than just wire and concrete.¹⁸⁵

In fact, defense in depth is increasingly being built around layered drone use.¹⁸⁶ In the security zone in Ukraine, a mix of ISR and small attack drones (e.g., FPVs) hunt enemy assault teams. Closer to friendly lines, unmanned ground vehicles (UGVs) and remote weapons stations cover sectors of fire, allowing humans to remain concealed and in hardened positions while filling in gaps and conducting resupply and maintenance. Drone substitution for scouts and fire teams reduces the number of personnel exposed to enemy fire along the front line. To further increase survivability, soldiers carry radio frequency scanners to alert them to approaching enemy drones. This security zone is also littered with a mix of mines and complex obstacle belts that limit enemy mobility and provide opportunities for direct and indirect fire to neutralize any penetration.

For a recent example, consider the Surovikin Line that complicated Ukraine's counteroffensive in 2023.¹⁸⁷ The line was a layered Russian fortification system designed to trade space for time and then convert that time into attrition. Its role in blunting the 2023 Ukrainian counteroffensive came from the integration of deep minefields, trenches, anti-tank obstacles, preplanned artillery fires, persistent drone reconnaissance, and local counterattacks. Importantly, the system did not need to be invulnerable; it only needed to slow the attacker long enough for the reconnaissance-fire complex to strip away tempo, breaching capacity, and operational reach.

In that sense, the Surovikin Line was a contemporary expression of defense in depth, specifically within a drone-saturated battlespace. Obstacles channeled movement, drones and sensors exposed breaching attempts, artillery and loitering munitions punished concentration, and local reserves restored the line before Ukraine could consolidate tactical gains. This front, and firing points immediately behind it for mortars and tube artillery, remained littered with decoys that reduced the enemy's ability to conduct effective fire missions while also helping to reveal the points of origin for attacks, thereby also supporting counter-battery missions. Finally, multiple hot and cold firing positions populated the line, allowing units to quickly shift locations to prevent enemy counter-battery.

The front along the Surovikin Line was connected to supply lines via net-covered roads designed to limit drone attacks. Furthermore, Russian teams used intermittent supply pushes when weather and light conditions limited or degraded operations. This allowed Russian tactical and operational reserves to stay further back from the front, increasing their survivability and capacity to launch counterattacks in the event of enemy breakthroughs or spoiling attacks in the event the enemy starts to mass.

This Russian staging area was also where medium-range air defenses protected the airfields and ammunition depots required to sustain operations along the front. When conditions permitted, aviation missions provided a mix of fires (e.g., close air support and interdiction) and defensive patrols to deny airspace to enemy air and drones. Yet, missions were limited in time and space given the density of Ukrainian air defenses. Combat missions were further constrained by the need to constantly reposition Russian aircraft to avoid long-range strikes by ballistic missiles often difficult to intercept or whose salvo size exceeded Russian interceptors.

This portrait of a modern, drone-enabled defense in depth is a harbinger of what NATO forces would likely confront in a Baltic scenario. After attacking, Russian forces would quickly tie into terrain and create a series of strong points, obstacle belts, and engagement areas designed to blunt any counterattack.

Case Study: NATO's Eastern Flank

NATO's primary operational concern on its eastern flank is the threat of a rapid *fait accompli* attack in which Russia seizes vulnerable allied territory and immediately transitions to a fortified defense in depth before the alliance can reach a political consensus and mobilize a unified military response.

This scenario has been discussed in recent literature. In one scenario, Russian forces launch an attack on an Estonian border city such as Narva using unmarked forces and proxies to seize key government offices and communications nodes, coupled with EW and standoff strikes to suppress Estonian C2 and air defenses. Aiming to present NATO with a *fait accompli*, Russia would drive at least 100 km inland in the first 48 hours while calling for ceasefires and mediation to stall the political consensus within NATO needed to invoke Article 5.¹⁸⁸

Another scenario envisions a more escalated attack, where Russia launches a two-pronged assault from Kaliningrad in the west and Belarus in the east to take control of the Suwalki Gap as quickly as possible, cutting off the Baltic states' land connection with the rest of the alliance. Russian forces would then entrench behind mines, obstacles, and extended air defense coverage to blunt any counterattack, buying time to create a new status quo and threatening nuclear escalation to further deter NATO before it can generate the mass necessary to retake the corridor.¹⁸⁹

Once entrenched, the adversary would transition to the defense and leverage a dense A2/AD network to make any NATO counteroffensive increasingly costly in blood and treasure. This campaign would seek to fracture political will and force a negotiated settlement that alters the European security architecture. The problem is speed. Russia would try to seize ground quickly, dig in, and make NATO's counterattack politically and militarily costly.

One of the most likely locations for a Russian incursion is the aforementioned Suwalki Gap.¹⁹⁰ This roughly 65 km (40 mile) stretch of border between Poland and Lithuania is the only overland corridor connecting the three Baltic member states—Estonia, Latvia, and Lithuania—to the rest of NATO by land. Flanked by the heavily militarized Russian exclave of Kaliningrad to the northwest and the staunch Russian ally Belarus to the southeast, the Suwalki Gap is characterized by flat, sparsely populated terrain and limited infrastructure, with only a couple of key roads and a rail line linking Poland to Lithuania.

Figure 24: The Suwalki Gap

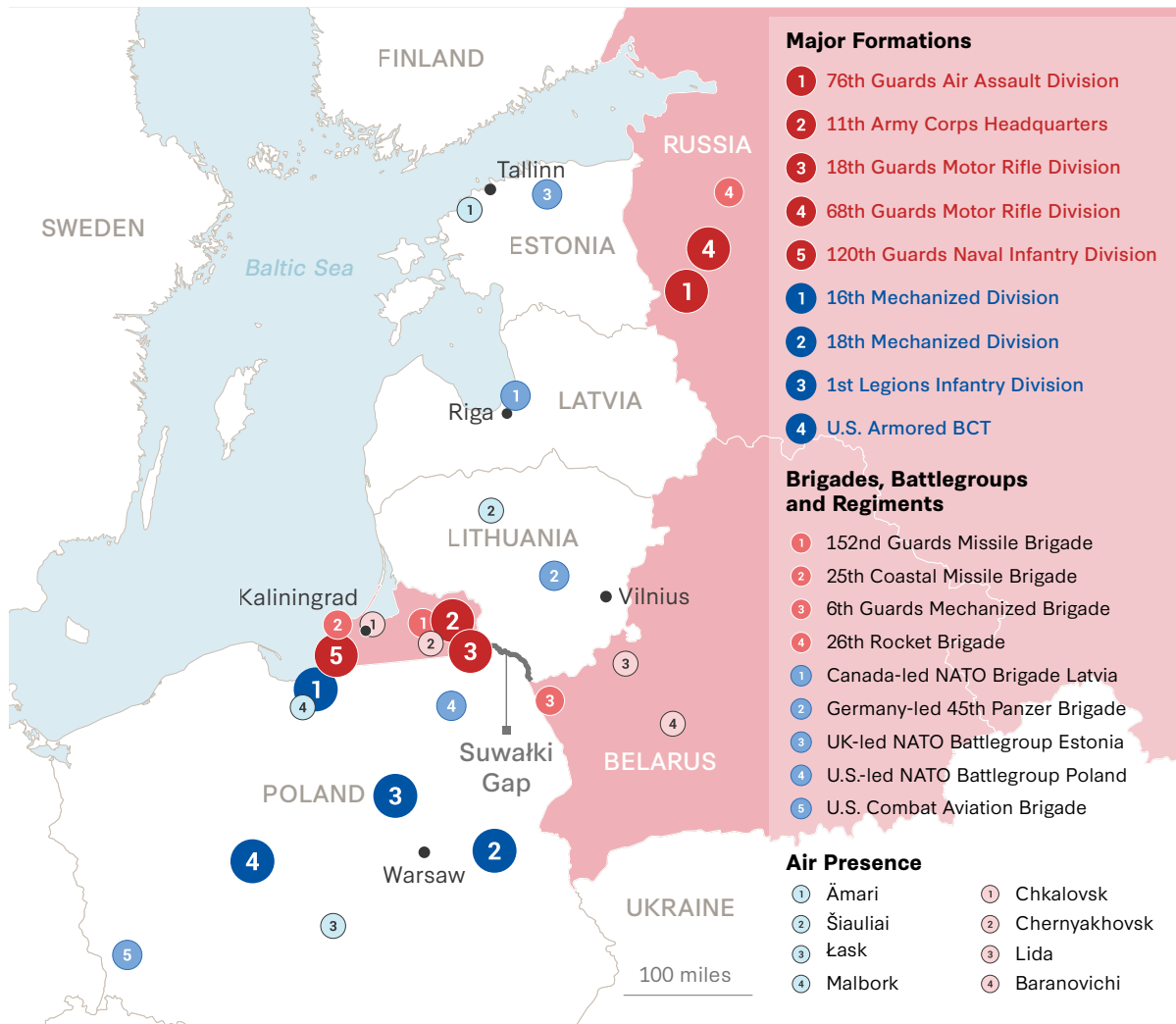


Source: Eric Rosenbach et al., *Russian Threats to NATO's Eastern Flank: Scenarios, Strategy, and Policy for European Security* (Cambridge, MA: Belfer Center for Science and International Affairs, February 2026), 8, https://www.belfercenter.org/sites/default/files/2026-02/Belfer_Russian%20Threats_3.1.pdf.

Past studies have consistently highlighted the extreme vulnerability of this geography and the logistical nightmare it presents for NATO. A seminal 2016 RAND wargame and subsequent study concluded across multiple scenarios that Russian forces could reach the outskirts of the Baltic capitals of Tallinn and Riga in as little as 36-60 hours, especially once they closed the gap.¹⁹¹ Subsequent studies highlighted a condition of “localized overmatch.”¹⁹² Specifically, while NATO possesses broader aggregate strength, Russia maintains both a significant time-distance advantage and a local superiority in heavy armor, mechanized infantry, and tactical fires along the immediate border. Furthermore, analysis by the Center for European Policy Analysis emphasized that Russia’s overlapping A2/AD bubbles from Kaliningrad and Belarus would turn the narrow Suwalki corridor into a severe operational trap for heavy, slow-moving NATO relief forces.¹⁹³ More recent scenario-based studies continue to stress that Russia’s larger strategy would be to achieve a fait accompli land grab before NATO could reach a political consensus.¹⁹⁴ As a result, the country’s operational approach would be to attempt to seize the gap in order to isolate the Baltics.

To understand the challenge of breaking this line, one must understand how Russia will fight. The Russian way of war relies on the doctrinal concept of *Aktivnaya Oborona* (Active Defense), which blends offensive preemption with deep, layered defensive operations designed to degrade an attacker before launching decisive counterstrikes. As observed in Ukraine, modern Russian operations integrate traditional massed fires with their modernized reconnaissance-fire complex. In this system, pervasive ISR drones (e.g., Orlan-10 and Supercam) are digitally linked to responsive fires and loitering munitions (e.g., ZALA Lancet, Molniya), reducing artillery kill-chain latency to minutes.

Figure 25: Baltics Map with NATO and Russian/Belarusian Forward Units



Source: CSIS Futures Lab.

Based on lessons learned from Ukraine, any Russian land grab would likely include the following lines of effort. First, there would be significant strategic signaling.¹⁹⁵ Russia, just as it did in Ukraine, would threaten nuclear escalation to limit NATO response options while also signaling the risk

of offensive action in space as well as wild claims about super weapons and attacks using “new physical properties” as a form of reflexive control. The desired effect would be to limit NATO response options to strictly proportional conventional strikes in an isolated geographic area.

Second, Russia will set conditions for any attack with a prolonged gray zone phase that includes deploying a mix of sleeper agents and criminal elements hired on the dark web to conduct sabotage operating alongside drones launched from shadow fleet vessels and clandestine elements. These missions will focus on degrading rail lines and other transportation corridors to compound regional isolation. Furthermore, Russian setting conditions will involve cutting fiber-optic cables and launching cyberattacks and propaganda campaigns that slow the ability of NATO to mobilize a counterattack force.

Third, Russia will initiate any attack with a large missile and drone offensive (i.e., firepower strike) designed to attrite enemy air defenses and limit the ability of forward-deployed NATO forces to move into battle positions. Like the firepower strikes seen in Ukraine, however, Moscow will saturate the front lines with drones to set conditions for ground forces to seize objectives and rapidly transition to the defense.¹⁹⁶ This would include swarms of low-cost systems such as the Molniya system and a fires complex built around the Lancet’s one-way attack and Zala-16 scouting drones, as well as glide bomb strikes once surface-to-air systems were neutralized.¹⁹⁷

With NATO forces thus isolated and scattered along the front lines, Russia would launch a combined arms assault using artillery integrated with loitering munitions and small drones to create maneuver corridors for its mechanized forces. The goal would not be a breakout in the traditional form of deep operations, but rather a more restricted movement designed to seize key terrain and transition to the defense in order to blunt any counterattack and buy time for negotiations.

Once key terrain in the Suwalki Gap is seized, Russian forces would rapidly engineer a multi-echeloned defensive bastion, drawing directly on the Surovikin Line constructed in southern Ukraine in 2023.¹⁹⁸ They would likely build a layered defense with mines, drones, EW, artillery, and reserves. This defense in depth expands doctrinal minefield depth from 100 m to over 200 m, utilizing remote mine-laying systems (e.g., ISDM Zemledeliye) to create complex obstacle belts and concrete “dragon’s teeth” anti-tank traps.¹⁹⁹ In its security zone, tethered ISR drones, acoustic sensors, and dense localized EW umbrellas (e.g., Pole-21 and Zhitel systems) would jam NATO communications and GPS.²⁰⁰ Thousands of FPV drones would be integrated into the defense, operating as a ubiquitous, dynamic aerial minefield capable of hunting NATO assault teams from the top down despite pilots located in secure remote locations. The area would also be integrated with preregistered artillery kill zones to create a robust engagement area. Behind the security zone, entrenched Russian infantry and mobile operational reserves—including Ka-52 attack helicopters alongside armor and mechanized battalions—would wait to counterattack any NATO penetration.

SET CONDITIONS

To break this defense in depth integrating EW and drones, NATO must orchestrate a decentralized swarm that bypasses the enemy’s frontal strength, penetrates its EW umbrellas, and breaks

defensive lines from within. Setting conditions requires a deliberate effort to sense, preposition, and deceive, ensuring the environment is prepared for a multi-axis swarming operation.

First, NATO must aggressively sense and map the Russian multilayered defensive web as it takes shape. Because the Russian reconnaissance-fire complex rapidly targets traditional reconnaissance assets, NATO must rely on high-altitude standoff sensors, clandestine cyber reconnaissance, and low-signature autonomous platforms to conduct its signal surveys. Planners then must map the signals pattern of life, identifying the data links connecting Russian operators to drones, geolocating EW jammers, and differentiating active artillery firing points from the myriad of thermal and physical decoys likely to litter the battlefield.

Simultaneously, OPE and AFOs would need to focus on building a resilient, distributed logistics web capable of sustaining NATO swarms conducting any counterattack. Recognizing that centralized staging areas in Poland will be targeted by Russian Iskander missiles and long-range drones, allied SOFs would need to infiltrate the periphery of the gap. Here they would establish concealed caches of containerized launched effects, ground-launched loitering munitions, UGVs, and battery recharging hubs along with relays and decoys. This prepositioning ensures the swarm can be generated from dispersed, unpredictable vectors within the contested zone, bypassing the need for vulnerable, road-bound supply convoys.

Finally, NATO planners would employ multidomain tactical deception. By projecting phantom C2 signatures, deploying electronic decoys, and simulating heavy-armor radio traffic along false axes of advance, NATO would force Russian commanders to unmask hidden artillery batteries, commit their defensive FPV screens prematurely, and shift mobile reserves away from the true intended breach points.

PULSE

With the defense mapped and the adversary manipulated, NATO forces would then initiate the first phase of the pulse, utilizing swarms to shape the battlespace and validate the kill web. This initial pulse functions as an aggressive, distributed sense-and-pull infiltration reminiscent of the Kursk operation in 2024.

Waves of low-cost, attritable UGVs and small UASs then push into the Russian security zone, deliberately triggering the defensive tripwires. As these expendable nodes encounter Russian remote weapons stations, minefields, and localized FPV screens, they force the enemy's active defense to radiate and engage. This action weaponizes the noise-to-signal ratio against Russian forces, while also validating the intelligence gathered during the sensing phase and confirming the locations of active drone hubs and hot firing positions. When an autonomous node discovers a seam in the extended remote minefields or an area where Russian EW coverage is degraded, it passes the target-quality track back to the network. Effectively executing reconnaissance pull, the swarm finds the gaps and signals the heavier, lethal elements to flow through the path of least resistance.

Once the Russian battle network is stimulated and the gaps are validated, the main pulse will commence. A heterogeneous swarm of loitering munitions, EW-equipped drones, and

precision-guided joint fires converges on the identified Russian weak points. Instead of attempting a grinding, linear breach through 500-meter-deep obstacle belts and dragon's teeth—which plays directly into Russian defense doctrine and places NATO forces squarely into artillery kill zones—the swarm targets the C2 and logistical nodes of the defense.

EW drone swarms then flood the local spectrum, severing and confusing the command links between Russian operators and their defensive UGVs and wireless FPV screens. Simultaneously, swarms of loitering munitions bypass the outer minefields to strike the identified drone-pilot trenches, counter-battery radars, medium-range air defense radars (e.g., Buk-M3), and hot artillery positions.

The goal of this phase is the disintegration of the enemy's defensive system. Confronted by waves of low-cost drones that strike simultaneously across the physical, informational, and human dimensions, the rigidly hierarchical Russian local command structure becomes paralyzed. This creates a temporary window for NATO mechanized infantry and armor to punch through the Russian line without facing devastating top-down drone strikes or preregistered artillery barrages.

CONSOLIDATE AND TRANSITION

Having ruptured Russia's defensive belts, NATO would need to rapidly consolidate its gains to prevent culmination and transition into an operational pursuit. The breached corridors shift from attack zones to support zones. As NATO's joint combined arms maneuver forces funnel through the cleared lanes in the Suwalki Gap, they are highly vulnerable to the doctrinal Russian counterattack.

To protect its forces, NATO would need to establish a localized defensive canopy comprising a forward-deployed mix of mobile C-UAS systems, localized EW jammers, and short-range air defenses to shield the refitting swarm nodes and heavy armor from any surviving Russian Lancet strikes or aviation sorties. At the same time, the fire support coordination line would need to be shifted eastward, opening the airspace for deep strikes and allowing NATO HIMARS and air power to target deeper echelons without risking fratricide.

Instead of pausing tempo, this consolidation serves as a springboard for the final transition. Anticipating the inevitable counterattack by Russian tactical and operational reserves, NATO will launch a secondary swarm—acting as a modern advanced guard—ahead of the main body to execute a mobile fires ambush. Sentinel nodes, including acoustic sensors, sleeper drones, and top-attack loitering munitions, would be deployed along the net-covered roads and forested avenues of approach leading from the Russian rear echelon. When Russian mechanized battalions and Ka-52 attack helicopters leave their staging areas to plug the breach, they travel into a kill zone. The secondary swarm would slow or disrupt counterattacking forces before they reach the breach. By destroying Russian logistics, fuel trucks, and lead vehicles miles before they reach the front line, the swarm denies Russian forces the ability to restore defensive integrity. In addition, relentlessly harassing the adversary's ability to reorganize, the swarm converts a tactical breach into a disorganized rout, breaking the Russian defense in depth and restoring NATO's contiguous land corridor to the Baltics.

This whole effort would require surging logistics forward, including staging key materials before sending smaller, unmanned systems along protected routes to reduce the efficacy of remaining Russian strike systems. Because the new front line would likely be forward of caches established during the preparation phase, these logistical resupply packages, called speedballs, would need to be prepackaged based on predictive analytics to reduce the time it takes to generate follow-on swarms.²⁰¹

Conclusion

The NATO eastern flank vignette illustrates how the swarming operational framework can break a modern defense in depth by disintegrating the reconnaissance-fire complex before heavy formations commit to a breach. NATO sets conditions by mapping mine belts, EW coverage, drone hubs, artillery firing points, command links, and reserve routes. Distributed caches and deceptive signatures position the swarm while pulling Russian forces away from the true breach. The opening pulse uses expendable UGVs and SUAS to stimulate the security zone, validate seams, and conduct reconnaissance pull. The main pulse then converges EW, loitering munitions, and joint fires against the nodes that give the defense cohesion: command posts and logistics. Once the system loses coherence, combined arms forces pass through the corridor. NATO consolidates and transitions by protecting the breach with mobile air defense and C-UAS, shifting the fire support coordination line forward, and using a secondary swarm to ambush reserves. The operational aim is to preserve tempo from penetration through pursuit.

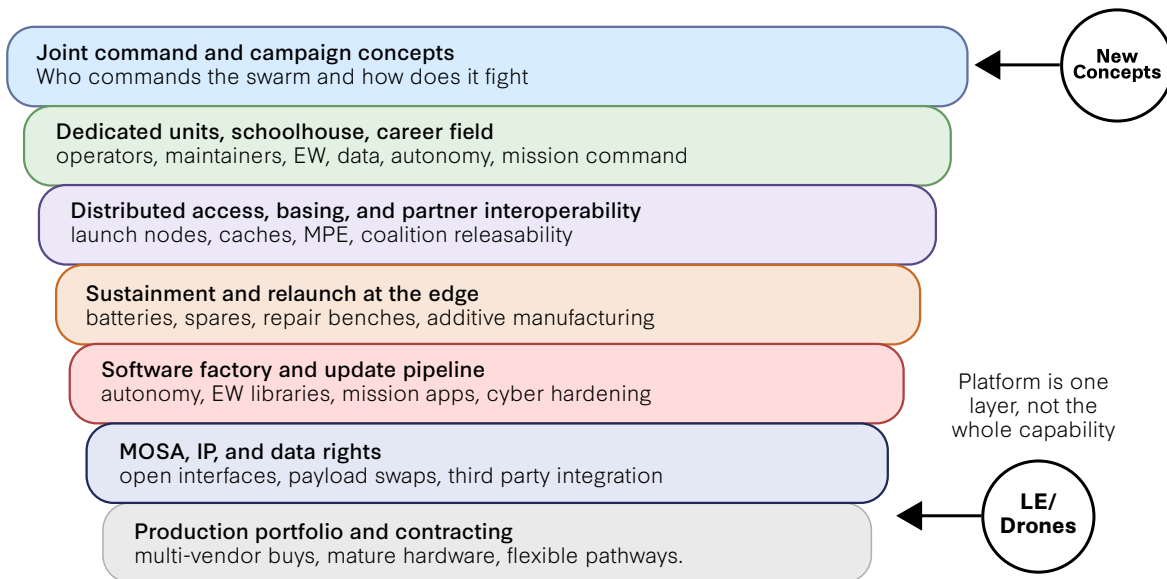
This concept places requirements on force design and sustainment that extend beyond buying more drones. NATO needs dedicated swarming formations with organic reconnaissance, EW, targeting, launch, recovery, repair, and data-exploitation (i.e., processing, exploitation, and dissemination [PED]) capacity. It also needs prepositioned containers, concealed charging and rearming sites, common mission-planning tools, and speedball resupply packages built around predictive demand. Coalition networks must pass target-quality tracks across national systems while operating under jamming and cyberattacks. Commanders need explicit transition criteria tied to corridor survivability, swarm attrition, enemy reserve movement, and the time required to regenerate the next pulse. These requirements point toward common components, rapid software updates, distributed logistics, and partner-ready interfaces. They also require recurring exercises that connect swarms to engineers, fires, air defense, and maneuver units.

Recommendations

The operational vignettes examined in this study point to a common conclusion. Swarms require a clear operational logic to become decisive. An acquisition strategy without operational art is a false promise. The value of swarms depends on whether the joint force can generate repeatable—and affordable—precision mass, impose disorientation, and then sustain the next pulse before the adversary recovers. That requires broader reforms that combine funds under single entities such as the DAWG and DRPM-UxS with building and testing entirely new concepts. The recommendations that follow translate this report’s operational logic into acquisition, software, basing, sustainment, interoperability, and force design choices. They focus on how to buy launched effects in meaningful numbers, preserve competition and adaptability, connect swarms to allies and combatant commands, and build the units, career fields, and command structures needed to effectively employ swarms in wartime. This overarching approach starts with operational concepts for employing swarms that connect new Pentagon acquisition efforts with combatant command and service concepts.

An acquisition strategy without operational art is a false promise.

Figure 26: More than Numbers: Swarms Require an Enterprise



Source: CSIS Futures Lab.

1. Build standing joint swarming task forces and campaign concepts for the combatant commands.

The Pentagon should build standing joint swarming task forces or, at a minimum, create designated joint swarming cells within key combatant commands and include those cells in major exercises. The purpose of the swarming cells would be to create new campaign concepts based on available launched effects and drones. Headquarters with such cells should rehearse how swarms support corridor opening, maritime scouting, deception, SEAD, target relay, counter-logistics, and pursuit operations. They should also own the practical work of target data exchange, airspace deconfliction, emissions control, coalition integration, and pulse regeneration. The gold standard for this initiative is the new Autonomous Warfare Command in United States Southern Command.²⁰²

This recommendation closes a critical policy gap. Force design is currently moving faster than doctrine and the ability of services to man, train, and equip swarm-capable formations. Ukraine's shift toward Drone Line and integrated drone-assault units, along with Russia's drive to stand up dedicated unmanned troops, reinforces the above conclusion that the side that operationalizes swarming through standing formations and repeatable headquarters processes—and does so more quickly than its adversary—gains an advantage.²⁰³ U.S. combatant commands need their own swarming playbooks, exercise series, and command relationships before crisis onset. Congress should ask not only how many launched effects the services are buying but which headquarters will command swarms, how quickly they can generate pulses, and what common standards govern their employment with allied forces.

2. Direct the services to create dedicated swarming units instead of treating drones as an accessory capability.

Buying more launched effects and drones will not produce swarming unless the services build formations whose primary task is to plan, launch, command, recover, rearm, and reconfigure swarms under combat conditions. In 2026, most U.S. units simply attach small unmanned systems onto existing aviation, infantry, or maritime organizations as an added duty. While that model can support experimentation, it rarely produces the repetition, tactical learning, or sustainment discipline needed to generate successive pulses at scale. Each service should therefore stand up dedicated swarming units with organic mission planning, launch and recovery teams, payload integration, EW support, data exploitation, and field repair. For the Army, that may mean battalions aligned to corps and divisions. For the Marine Corps, it could be formations tied to Marine littoral regiments and expeditionary forces. For the Air Force and Navy, this might entail dedicated squadrons, detachments, or expeditionary cells that can plug into air and maritime component commands without being improvised in crisis.

Ukraine has already moved in this direction. In February 2024, President Volodymyr Zelenskyy announced that Ukraine would establish the Unmanned Systems Forces as a separate branch.²⁰⁴ Kyiv then used the Drone Line initiative to build and scale the most effective unmanned units across the force and, in April 2026, described a new combat model built around drone-assault units that combine aerial and ground unmanned systems with infantry in a single formation.²⁰⁵ Russia is moving in a similar direction. In June 2025, Putin announced that Russia was creating unmanned systems troops as a separate branch, and subsequent reporting showed Moscow recruiting dedicated operators and engineers for drone units while expanding specialist formations.²⁰⁶ The broader lesson is that both combatants are growing unmanned formations faster than most legacy combined arms organizations can be redesigned. The United States must, at a minimum, follow suit, if not take the lead, in integrating dedicated swarming forces within the services. To that end, Congress should require each service to present a force design plan for swarming in its next budget cycle, including unit types, readiness metrics, and how those units support combatant command campaign plans.

Congress should require each service to present a force design plan for swarming in its next budget cycle, including unit types, readiness metrics, and how those units support combatant command campaign plans.

3. Create a professional swarming career field, schoolhouse, and command track.

Dedicated units will fail without a profession to man them. The services need a recognized swarming career field that combines operators, mission commanders, autonomy software integrators, EW specialists, maintainers, and data analysts. As of mid-2026, too much U.S. drone talent remains organized as borrowed labor from other branches, resulting in short tours, weak continuity, and constant relearning. Each service should create a formal training pipeline from entry-level operator to advanced swarm mission commander, with common joint modules in autonomy, emissions discipline, C-UAS, human-machine teaming, and re-attack cycles. The aim is to produce officers, noncommissioned officers, and civilians who can command a swarm as a tactical system and keep it adapting in contact.

Ukraine's education and training reforms illustrate what serious adaptation looks like. In 2025, the Ukrainian Ministry of Defence expanded its higher military education for operational, tactical, maintenance, repair, and command specialties tied to unmanned systems. In 2026, it reported an established network of certified training centers and more than 5,000 UAS operators trained in a single year.²⁰⁷ Russia is also recruiting students and engineers directly into drone units and building dedicated training and doctrinal representation for its unmanned branch. The United States should not wait for a crisis to discover that swarming is a manpower problem as much as a procurement problem. Congress and the Pentagon should examine whether existing bonus, civilian hiring, reserve affiliation, and lateral-entry mechanisms are sufficient to attract the coders, roboticists, technicians, and tacticians these units will need.²⁰⁸

Congress should require the Pentagon to identify which access agreements, storage permissions, and sustainment arrangements are in place to support swarms by combatant command.

4. Build cooperative security locations and preposition swarm nodes across multiple combatant commands.

Swarms become operationally relevant only when they can be launched from dispersed, hard-to-target locations close enough to matter. The Pentagon should therefore use theater-level campaign plans and security cooperation mechanisms to build a network of small-footprint, cooperative security locations, cache sites, and partner-operated launch and recharge nodes across multiple combatant commands. Pentagon policy already states that security cooperation should be used to develop allied and partner capacity and to provide U.S. forces with peacetime and contingency access to host nations.²⁰⁹ This is the right policy scaffolding for containerized swarm kits, battery hubs, maintenance benches, data update points, and mission-planning enclaves distributed throughout the Indo-Pacific, Europe, and selected locations in the Middle East and Africa.

The key to successful implementation is resisting the temptation to turn launched effects into another large base program. A swarm architecture based on containerized effects should be tied to a distributed access strategy, not to a few large hubs that invite missile attack. Legislatively and politically, this recommendation raises real issues: Title 10 versus Title 22 funding boundaries, host-nation approvals, explosive storage and force protection rules, environmental and safety constraints, and the question of whether a site is merely a training and access node or effectively a prepositioned war reserve facility, to name a few. Congress should require the Pentagon to identify which access agreements, storage permissions, and sustainment arrangements are in place to support swarms by combatant command. Without that map, swarms will remain a paper capability that cannot survive the first salvos of a real campaign.

5. Make partner interoperability a threshold requirement and treat “PIPIR-type” networks as mission-partner environment problems.

Swarms should be interoperable with allies. The applicable doctrinal and policy anchor is the Mission-Partner Environment, which the Pentagon’s Instruction 8110.01 defines as the operating framework that enables C2 and information sharing across the full range of military operations and requires the use of common standards, protocols, and interfaces compatible with mission partners and Federated Mission Networking specifications.²¹⁰ For launched effects, that means releasable mission planning data, shared deconfliction rules, coalition payload status reporting, compatible data transport, and a partner-ready logistics picture.

Congress should require that the Pentagon create coalition interoperability plans for swarming-capable drones and launched effects.

Furthermore, this entails building coproduction and partner assembly around common interfaces rather than around bespoke national variants that cannot be integrated under pressure. That means building on existing frameworks such as AUKUS Pillar II and the Partnership for Indo-Pacific Industrial Resilience.²¹¹ There is a web of agreements already in place to support building swarms with partners. Congress should require that the Pentagon create coalition interoperability plans for swarming-capable drones and launched effects. This plan should include what data is releasable, how the coalition will create a common operating picture, and how partner-built variants will remain electrically and digitally interoperable with U.S. launch, control, and sustainment systems.

6. Standardize common components across the services to deepen supply systems.

The Pentagon should establish a joint commonality list for launched effects and related swarm systems. Common modules in particular allow distributed swarms to reconfigure quickly and generate precision mass without becoming logistically brittle. Translating that into procurement procedures entails standardizing what can reasonably be standardized: batteries and power management modules, launch-tube dimensions, data links, ground-control tablets, payload modules, recovery kits, and container dimensions. The Pentagon's industrial strategy moves toward supporting this logic by prioritizing resilient supply chains, flexible acquisition, and deeper allied and partner industrial collaboration, but it must be extended to swarm-capable drone systems.²¹² They can also negotiate and acquire the rights to develop alternative sources of supply and manufacture when necessary, easing the challenge of purchasing common components across services.²¹³

Congress should direct the Pentagon to publish a joint launched effects and drone roadmap for common components.

Congress should direct the Pentagon to publish a joint launched effects and drone roadmap for common components and an annual report on where cross-service divergence is justified and where it is simply a self-inflicted logistics penalty.

7. Build distributed sustainment, repair, and additive manufacturing support around swarms.

Swarm operations are won or lost in the transition between launches. The Pentagon should develop a distributed sustainment concept that treats batteries, repair parts, and payload swaps as part of an integrated system. Joint logistics doctrine puts special emphasis on resilience, responsiveness, visibility, and the integration of commercial capabilities and partner support.²¹⁴ The defense industrial strategy also explicitly calls for resilient supply chains, strategic stockpiles, diversified suppliers, and modernized production methods.²¹⁵ For swarming systems, this should translate into containerized repair benches, common tools, field-level diagnostics, and additive manufacturing options for selected non-sensitive parts.

Congress should require the Pentagon to define which launched effects and drone components can be repaired at the tactical edge, which require depot intervention, and which can be 3D printed safely and legally in theater. A “mass” capability that cannot survive attrition, recharge, reload, and relaunch at the edge will collapse after the first battle.

8. Mandate a modular open-systems architecture and government-controlled update paths.

Modular Open Systems Approach (MOSA) is a key requirement for supporting swarming formations. Open interfaces support swapping payloads, updating software, and integrating allied systems without relying on one vendor. Title 10 already requires that defense acquisition programs, to the maximum extent practicable, use MOSA, specifically to enhance competition, innovation, and interoperability.²¹⁶ Related statutory provisions require that major system interfaces be designated, documented, and delivered with the technical information necessary for third-party integration.²¹⁷ For launched effects specifically, this means that every solicitation should require open and machine-readable interface control documents, published application programming interfaces where appropriate, modular mission computer boundaries, and delivered documentation sufficient for government and third-party integration of payloads and mission planning tools.

The second half of the solution comprises data and software rights. Under 10 U.S.C. § 3771, the government can and should secure government-purpose rights in modular-system interface technical data, even where mixed funding or private expense is involved, subject to appropriate compensation rules.²¹⁸ The Pentagon cannot update autonomy logic, re-task payloads, harden cyber defenses, or complete subsystem replacements at speed if the interfaces are proprietary black boxes. To this point, its newly released Intellectual Property Guidebook exists precisely to help acquisition professionals build this kind of strategy.²¹⁹ Legislatively, Congress should insist that swarm-capable launched effects programs submit an explicit intellectual property (IP) and MOSA strategy before major production decisions and identify which interfaces and government-hosted build or deployment rights are essential to avoid vendor lock.

9. Create a joint launched effects software factory and a continuous update pipeline.

A swarm that cannot be updated quickly will be defeated quickly. Software for mission planning, EW, and autonomous flight and navigation should be managed through a joint software factory ecosystem rather than through slow, hardware-centric release cycles. The Pentagon's Software Modernization Implementation Plan calls for a department-wide software factory ecosystem, continuous authorization to operate, enterprise licensing, and the removal of barriers to operating in cloud-enabled development environments.²²⁰ These guidelines are directly applicable to launched effects and swarming drones, where the value depends heavily on how fast the software layer can be adapted to adversary countermeasures. What is unclear is if existing acquisition programs such as DAWG and DRPM-UxS are tackling the software challenge.

The policy implication is that procurement alone will not solve the problem. The Pentagon must budget for software updates. Every launched effects and swarm family should have government-approved continuous integration and deployment pathways, exportable software baselines for partners, and clear release authorities for autonomy changes. Congress should ask a simple question during oversight: How long does it take to update

mission software across the fleet and push the change to operational units and partners? If the answer is measured in months rather than days, the system is still operating like a legacy program rather than like a modern swarm enterprise.

10. Establish joint portfolio governance, common operational measures, and a recurring cross-service test campaign.

The Pentagon should also create a joint launched effects portfolio governance mechanism with real authority over standards, testing, and operational measures. In theory, this is exactly what the new DRPM-UxS should accomplish. The purpose would be to prevent the services from fielding mutually incompatible effects that cannot converge in a joint fight.

The Army's FY 2026 budget materials already describe launched effects as part of a broader agile development and rapid prototyping effort.²²¹ This effort should be linked to swarming effects and A2/AD penetration outlined in the scenarios above. It should include transition criteria based on sensor suppression, attrition, corridor survivability, and regeneration capacity. That logic should become part of a common joint measurement framework, whether in DAWG or the larger DRPM-UxS.

Whatever form the overarching governance and procurement framework takes, it needs to be paired with recurring cross-service operational test campaigns that evaluate swarms against likely operational challenges similar to the scenarios used in this report. For example: How quickly can a swarm open an air or ground maneuver corridor? How quickly can it regenerate a second pulse in a contest over sea control in the first island chain? How effectively can it integrate with follow-on fires and allied systems? In addition, tests should evaluate the swarm's capabilities to open a window, survive contact, and generate the next pulse. Congress can help without overcentralizing by requiring an annual review. The review should report on major operational scenarios.

11. Increase purchases of launched effects and swarm-capable drones through an operationally meaningful, multivendor portfolio.

The Pentagon should move immediately from demonstration quantities to operationally meaningful buys of launched effects families that are already being evaluated for fielding. The Army has already selected AEVEX's Atlas, Anduril's ALTIUS-600, and Raytheon's Coyote Block 3 for LE-SR demonstrations, and Army program officials now describe launched effects as a family of systems intended to enhance maneuver across air and ground domains.²²² At the same time, the Army's FY 2026 budget materials show dedicated agile-development funding for future UAS air-launched effects and note that rapid prototyping began in 2026 and is expected to finish by 2030.²²³

Seen in this light, efforts such as DAWG and DRPM-UxS are promising as long as they align resources and authorities. Purchases should be portfolio-based, not winner-take-all. A single-vendor monopoly would reduce competition, slow adaptation, and potentially create a brittle supply chain. The better model is a standing portfolio with recurring orders for platforms, payloads, launchers, and support kits, all tied to common interface rules and

operational test results. Replicator’s emphasis on fielding thousands of autonomous systems and lowering barriers for traditional and nontraditional firms echoes this assessment.²²⁴

The legislative concern centers on the appropriations structure. To ensure that the Pentagon does not continue hiding program growth inside scattered accounts, Congress should demand a visible launched effects and swarming-capable drone portfolio line with separate wedges for procurement, software, and experimentation.

Last, the purchases must be linked to a clear family of operational concepts for employing affordable mass. As outlined in this report, this framework should consider how to restore the offense on a modern battlefield dominated by low-cost, proliferated sensors that favor the defense. New initiatives such as DAWG and DRPM-UxS should align with service and combatant command experimentation to build on concepts such as the one outlined in this report.

12. Expand flexible contracting options for payloads, software, and support kits.

Launched effects and swarming-capable drones should be bought under contracting structures that match the technology’s rapid development pace. The most useful tools for purchase are Other Transactions follow-on production and multiple-award indefinite-delivery/indefinite-quantity vehicles that let the government order air vehicles, payloads, autonomy software, and support equipment separately.²²⁵ Whether those elements can actually be sourced independently depends on the modular architecture and interface rights discussed above. Congress already gave the Pentagon wide latitude in 10 U.S.C. § 4022 to prototype commercial and agile-development solutions and then transition successful prototypes into follow-on production.²²⁶ The Army is already exploiting streamlined pathways and Other Transaction Authority-based structures in its current launched effects work. The Pentagon should normalize that model across the services instead of treating it as an exception.²²⁷

Fast contracting without disciplined rules can produce vendor lock, unclear data rights, and non-repeatable sustainment. Therefore, every launched effect and swarm-capable drone prototype agreement, from the start, should include provisions for follow-on production, exportability planning, cybersecurity, and sustainment. Middle Tier of Acquisition authorities are especially useful here because statute and implementation guidance are built around rapid prototyping and fielding in two-to-five-year windows.²²⁸ Congress should encourage expanded launched effects use of these pathways, while also requiring services to document how each rapid acquisition action will transition into a durable program baseline instead of dying in the “valley of death.”²²⁹ In fact, Congress should ensure it aligns this type of review with existing subcommittees in the House and Senate Armed Services Committees.

13. Place mature launched effects families on a pathway to multiyear procurement.

Once specific launched effects platforms, motors, batteries, data links, and launch canisters reach stable configurations, the Pentagon should seek multiyear procurement authority for those mature baselines. The legal foundation already exists. Multiyear contracts are authorized under 10 U.S.C. § 3501 when they save money or stabilize the defense industrial base and when minimum need is expected to remain substantially unchanged.²³⁰ In practical

terms, this means the Pentagon should not wait until a launched effect is “finished,” because it never will be. Instead, it should identify the stable layers of the system that justify multiyear treatment and leave the unstable layers (e.g., software, autonomy behaviors, and some payloads) on faster refresh cycles.

Cutting across the entire swarm stack, the right candidate for multiyear procurement is the subset of recurring hardware whose design has stabilized enough to support economic-order quantities and predictable production rates. Motors, batteries, airframes, launch tubes, canisters, and common communications modules are better multiyear candidates than mission software or fast-changing EW payloads, for example. Congress should require the services to certify that any multiyear launched effects proposal is limited to stable baselines. It should be structured as a fixed-price procurement, where appropriate, and include a clear strategy for avoiding the classic failure mode that locks a rapidly evolving capability into a procurement profile that inhibits software and payload modernization.

14. Create an airborne layer to enable launched effects and swarm-capable drones.

The Pentagon should fund an airborne layer to enable swarms as uncrewed airborne nodes that can launch, relay, scout, and direct launched effects when orbital support is degraded or terrestrial networks are intermittent. Space will remain essential, but it will be contested.²³¹ Moreover, Pentagon reporting to Congress on Chinese military power continues to warn that Beijing is developing counterspace capabilities, jammers, and anti-satellite systems meant to deny U.S. access and operations within the space domain.²³² Swarming therefore cannot assume pristine satellite connectivity. It needs a responsive airborne layer that can restore line-of-sight control, extend kill chains, translate data across networks, and keep the pulse moving even when the orbital backbone is under pressure.

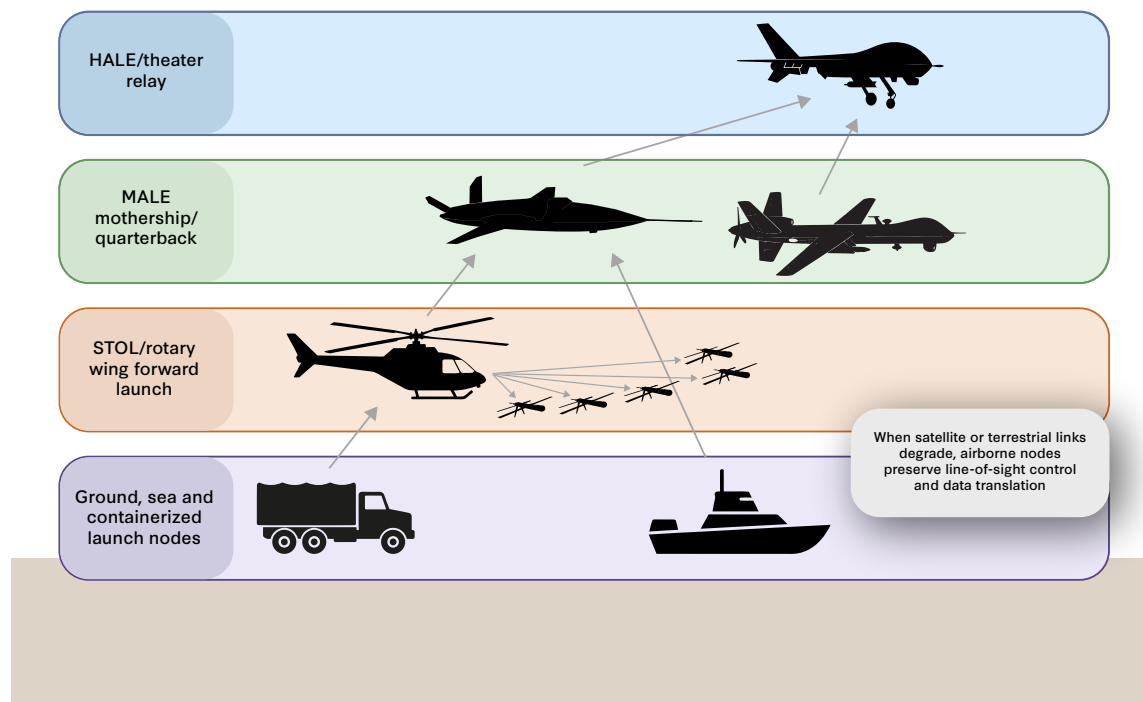
The airborne layer should be tiered. At the forward edge, helicopters and other low-altitude platforms should forward-launch launched effects from masked positions, especially since the Army has already demonstrated common launch solutions on the AH-64 and is integrating the same capability onto the UH-60.²³³ The U.S. Marine Corps is exploring similar options with the UH-1Y.²³⁴ Above them, medium-altitude long-endurance and high-altitude long-endurance unmanned systems should operate as motherships, armed scouts, and quarterbacks. Some platforms should carry additional launched effects, while others host EW, sensing, or targeting payloads. Others should serve mainly as airborne communications and data fusion nodes. The existing Battlefield Airborne Communications Node (BACN) model—a fielded Air Force airborne gateway that relays, bridges, and translates between otherwise incompatible tactical data links—shows what that quarterback function can look like. The BACN model provides a high-altitude communications gateway that bridges disparate air, ground, and maritime users but has been continually under threat as the U.S. Air Force cancels both platforms linked to it (EQ-4B and E-11A) in favor of hybrid SATCOM.²³⁵

To provide maximum flexibility, the Pentagon should invest in short takeoff and landing (STOL) or runway-independent variants of unmanned systems for this layer instead of assuming long, pristine runways will be available. The Army’s new Group 4+ STOL—an

initiative to field large, runway-independent drones—already points toward systems built for unimproved areas, network extension, and long endurance using MOSA.²³⁶ Manned options could include Air Force Special Operations Command’s OA-1K—a manned light-attack platform—that demonstrates the value of aircraft able to use austere fields and short takeoffs and landings.²³⁷ This logic aligns with the Agile Combat Employment doctrine, which starts from the premise that large fixed bases are increasingly vulnerable and that combat power must be generated from dispersed clusters and contingency locations under threat.²³⁸ Despite this recognized vulnerability, manned systems have significantly less dwell time than unmanned systems and, consequently, often shift the risk calculus in operational planning, creating a need to sustain legacy, medium-altitude long-endurance programs across multiple services.

In practice, an airborne layer will be most useful in theaters with dynamic Forward Lines of Own Troops (i.e., front line), damaged runways, fragmented communications, and rapidly shifting launch windows. Congress and the Pentagon should therefore treat this layer as a joint enabler instead of a service-specific platform. With that in mind, Congress should direct a joint concept demonstration and require a budget exhibit that tracks airborne launch, relay, and control capacity alongside launched effects procurement. In addition, the Pentagon should set common standards for airworthiness, weapons release, data links, emissions control, and coalition interoperability so that the airborne layer does not become another service-specific stovepipe.

Figure 27: Creating a Tiered Airborne Layer to Enable Launched Effects



Source: CSIS Futures Lab.

Conclusion

Modern battle networks make offensive concentration more dangerous, but they do not remove the need for massing effects. Instead, they change its shape and form on the battlefield. The United States will need a way to generate low-cost, precision mass without presenting dense, predictable formations to an adversary armed with cheap sensors, layered fires, and adaptive battle networks. In other words, the United States must be able to employ swarming as an operational form in future campaigns.

As the above scenarios revealed across Kaliningrad, the South China Sea, and NATO's eastern flank, the insights are consistent. Swarms help a joint force set conditions, deliver a pulse, and consolidate and transition before the defender can recover. They generate not just destruction but disorientation. They fracture how an enemy sees, decides, and reacts. In that context, launched effects are one of the most practical means emerging to field swarms at scale.

The Pentagon should resist governing swarms as a niche munition line or a collection of service-specific experiments and instead see them as a larger, joint operational system. That framing links procurement, contracting, technical standards, and data rights with access, basing, coalition interoperability, and sustainment. If one of those layers fails, the larger concept weakens. A swarm that cannot be bought in meaningful numbers is irrelevant. A swarm that can be bought but not updated will not adapt to a changing battlefield. And a swarm that can be updated but not sustained forward will lead to fragile campaigns and fleeting results.

The recommendations in this paper fit into four larger lines of effort:

1. **Scale swarm production.** The Pentagon needs to buy more launched effects and swarm-capable drones now, widen the vendor base, employ flexible contracting where speed matters, and lock in multiyear procurement for mature designs.
2. **Prevent lock-in and preserve adaptability.** The Pentagon and Congress should mandate the use of MOSA and build a joint software pipeline that treats updates as a recurring wartime requirement rather than an occasional program event.
3. **Make swarming usable in future campaigns.** The Pentagon will need to work with other government agents to identify cooperative security locations, preposition containers and caches, and enable mission partner connectivity. It will also need to prioritize common components across services, distributed repair and sustainment, and a recurring joint test architecture that measures whether swarms can regenerate the next pulse under pressure.
4. **Build formations and talent capable of fighting as swarms.** Without new formation and training pipelines, swarms are unlikely to take hold across the services. The Pentagon needs to create dedicated swarming units, career fields, schoolhouses, and joint task forces to develop and refine new concepts.

Congress and the Pentagon will also need to align oversight. Funding for launched effects and swarms should be visible rather than buried across disconnected research, rapid acquisition, and platform lines. Major production decisions should require credible MOSA and IP strategies, not promises to solve integration later. Multiyear procurement should apply to proven designs, while flexible contracting should support software or payload layers that need more frequent revision. Oversight should ask the questions most likely to matter in wartime: How fast can software and payload updates be fielded? How interoperable are systems across the services and with allies? How much commonality exists in critical components and supply chains? How resilient is forward sustainment? Are dedicated swarming units actually manned, trained, and ready?

Implemented correctly, efforts such as DAWG and DRPM-UxS have the potential to provide flexible systems capable of producing unmanned systems for distributed reconnaissance, deception, electronic attack, and strike options aligned with service and joint concepts. In the Kaliningrad scenario outlined above, that means helping to pry open corridors through an integrated air defense by forcing radars to radiate, stretching magazines, and attacking the connective tissue of the system. In the case of the South China Sea, it implies more scouting, creating false contacts, and generating local windows of maritime advantage without betting everything on one dramatic exchange. Finally, on NATO's eastern flank, it means helping rupture a defense in depth by sensing seams, manipulating the defender, and regenerating follow-on pulses before a counterattack can settle the fight. Crucially, these cases reveal that an operational approach to swarming needs new concepts, organizations, training pipelines, and support infrastructure. Those requirements extend beyond purchasing the right drone to building the right types of units, which takes time and focus across the services.

This effort to align drone portfolios with operational concepts will also require congressional oversight and reporting. The campaign will take years and taxpayer dollars beyond those programmed in current budgets. Congress has a clear oversight role to ensure that the Pentagon, regardless of what portfolio model emerges, aligns its investments in drones and swarm-capable platforms with a clear theory of victory and operational requirements. And this oversight responsibility must include looking for ways to maximize affordability, including MOSA and common components that reduce costs across service budget lines.

About the Author

Benjamin Jensen is director of the Futures Lab and a senior fellow for the Defense and Security Department at the Center for Strategic and International Studies (CSIS). At CSIS, Dr. Jensen leads research initiatives on applying data science and AI and machine learning to study the changing character of war and statecraft. Under his leadership, Futures Lab has pioneered building AI applications into wargames and innovative scenario exercises. The exercise topics range from major war, competitive strategy, and national mobilization to economic security, energy politics, and national resilience. He is also the Frank E. Petersen Chair for Emerging Technology and a professor of strategic studies at the Marine Corps University School of Advanced Warfighting (MCU). At MCU, he leads a research program on future war and teaches seminars on modern operational art and joint all-domain operations. Dr. Jensen has authored five books including *Information in War: Military Innovation, Battle Networks, and the Future of Artificial Intelligence* (Georgetown University Press, 2022), *Military Strategy in the 21st Century: People, Connectivity, and Competition* (Cambria, 2018), *Cyber Strategy: The Evolving Character of Power and Coercion* (Oxford University Press, 2018), and *Forging the Sword: Doctrinal Change in the U.S. Army* (Stanford University Press, 2016). He also served as senior research director for the U.S. Cyberspace Solarium Commission and is a reserve officer in the U.S. Army, with command experience from platoon to battalion. Dr. Jensen graduated from the University of Wisconsin-Madison and earned his MA and PhD from the American University School of International Service.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Founded in 1962, CSIS is led by General Joseph F. Dunford, who was appointed chief executive officer in 2026, succeeding John J. Hamre. The CSIS Board of Trustees is chaired by Thomas J. Pritzker, who has held the position since 2015.

CSIS brings together more than 275 full-time staff and a global network of affiliated scholars working across four core areas of public policy: defense and security, geopolitics and foreign policy, economic security and technology, and global development. Our scholars are regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer recommendations to improve U.S. strategy.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—non-partisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

What sets CSIS apart is not only the quality of its research but how that research is conveyed: through original data and open-source analysis; through multimedia and data visualization; and through connecting relevant analysis with key audiences at the moments that matter most. This combination of rigor, independence, and reach has made CSIS a driving force in the policy debates shaping American security and prosperity.

Endnotes

- 1 Anna Miskelley, “The Pentagon’s \$54 Billion Bet on Autonomous Warfare,” *Defense One*, May 22, 2026, <https://www.defenseone.com/ideas/2026/05/pentagons-54-billion-bet-autonomous-warfare/413735/>; and Mallory Shelbourne, “New Pentagon Unmanned Czar Will Oversee Most Drone Programs, Memo Reads,” U.S. Naval Institute, July 1, 2026, <https://news.usni.org/2026/07/01/new-pentagon-unmanned-czar-will-oversee-most-drone-programs-memo-reads>.
- 2 Barry D. Watts, *The Evolution of Precision Strike* (Washington, DC: Center for Strategic and Budgetary Assessments, 2013), <https://csbaonline.org/uploads/documents/Evolution-of-Precision-Strike-final-v15.pdf>; and Thomas G. Mahnken, “Weapons: The Growth & Spread of the Precision-Strike Regime,” *Daedalus* 140, no. 3 (2011): 45–57, https://doi.org/10.1162/DAED_a_00097.
- 3 “Sudan War Strategy Shifts to the Air as Both Sides Increase Drone Use,” *Africa Defense Forum*, July 15, 2025, <https://adf-magazine.com/2025/07/sudan-war-strategy-shifts-to-the-air-as-both-sides-increase-drone-use/>; Kathryn Tyson, “Drones Over Sudan: Foreign Powers In Sudan’s Civil War,” *Critical Threats*, January 27, 2025, <https://www.criticalthreats.org/analysis/drones-over-sudan-foreign-powers-in-sudans-civil-war/>; “Malian Insurgents Attack with Drones,” *Africa Defense Forum*, April 28, 2026, <https://adf-magazine.com/2026/04/malian-insurgents-attack-with-drones/>; “African Armies Turn to Drones with Devastating Civilian Impact,” *France24*, July 25, 2025, <https://www.france24.com/en/live-news/20250725-african-armies-turn-to-drones-with-devastating-civilian-impact>; “Suicide Drone Discovery in Somalia Signals Shift in Terror Tactics,” *Africa Defense Forum*, September 24, 2024, <https://adf-magazine.com/2024/09/suicide-drone-discovery-in-somalia-signals-shift-in-terror-tactics/>; Kateryna Bondar, “How and Why Ukraine’s Military Is Going Digital,” CSIS, white paper, October 6, 2025, <https://www.csis.org/analysis/how-and-why-ukraines-military-going-digital>; Kateryna Bondar, “Ukraine’s Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare,” CSIS, white paper, March 6, 2025, <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare>; Timothy Ditter, *PRC Concepts for UAV Swarms in Future Warfare* (Alexandria, VA: CNA Corporation, October 2025), <https://www.cna.org/analyses/2025/10/prc-concepts-for-uav->

swarms-in-future-warfare; Stacie Pettyjohn et al., *Swarms over the Strait* (Washington, DC: Center for a New American Security (CNAS), June 2024), <https://www.cnas.org/publications/reports/swarms-over-the-strait>; Stacie Pettyjohn, *Evolution Not Revolution: Drone Warfare in Russia's 2022 Invasion of Ukraine* (Washington, DC: CNAS, February 2024), <https://www.cnas.org/publications/reports/evolution-not-revolution>; and Aaron Barlow et al., “Supporting Evidence of the Precision Mass Thesis,” *War Quants*, January 19, 2025, <https://www.warquants.com/p/supporting-evidence-of-the-precision>.

- 4 Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret, with commentary by Bernard Brodie (Princeton, NJ: Princeton University Press, 1976); and Christopher Saunders, “Logic and Grammar: Clausewitz and the Language of War,” *The Strategy Bridge*, October 9, 2020, <https://thestrategybridge.org/the-bridge/2020/10/9/logic-and-grammar-clausewitz-and-the-language-of-war>.
- 5 On battle networks as a unifying theory of kill webs and kill chains, see Benjamin M. Jensen, Christopher Whyte, and Scott Cuomo, *Information in War: Military Innovation, Battle Networks, and the Future of Artificial Intelligence* (Washington, DC: Georgetown University Press, 2022); and Todd Harrison, *Battle Networks and the Future Force* (Washington, DC: CSIS, August 2021), <https://www.csis.org/analysis/battle-networks-and-future-force>.
- 6 Michael C. Horowitz, “Do Emerging Military Technologies Matter for International Politics?,” *Annual Review of Political Science* 23 (May 2020): 385–400, <https://doi.org/10.1146/annurev-polisci-050718-032725>.
- 7 Jon Sumida, “On Defense as the Strongest Form of War” (draft), *Clausewitz Studies*, March 15, 2005, <https://clausewitzstudies.org/hold2/Sumida-ClausewitzAndDefense.pdf>.
- 8 As quoted in Peter Dickinson, “Russia’s Retreat from Crimea Makes a Mockery of the West’s Escalation Fears,” *Atlantic Council*, July 16, 2024, <https://www.atlanticcouncil.org/blogs/ukrainealert/russias-retreat-from-crimea-makes-a-mockery-of-the-wests-escalation-fears/>.
- 9 Mark Temnycky, “Ukraine Has Innovated Naval Warfare,” *Center for Maritime Strategy*, July 31, 2025, <https://centerformaritimestrategy.org/publications/ukraine-has-innovated-naval-warfare/>.
- 10 Benjamin Jensen, “Operational Art in the Age of Battle Networks,” in *War and the Modern Battlefield: Insights from Ukraine and the Middle East* (Washington, DC: CSIS, September 2025), <https://www.csis.org/analysis/chapter-4-operational-art-age-battle-networks>; Angelica Evans, *Ukraine’s Kursk Incursion: Six Month Assessment* (Washington, DC: Institute for the Study of War, February 2025), <https://understandingwar.org/research/russia-ukraine/ukraines-kursk-incursion-six-month-assessment-2/>; Dan Cox, “The Operational and Strategic Genius of the Kursk Offensive,” *Foreign Policy Research Institute*, November 22, 2024, <https://www.fpri.org/article/2024/11/the-operational-and-strategic-genius-of-the-kursk-offensive/>; Ann Marie Dailey, “Ukraine’s ‘Masterstroke’ Kursk Offensive is About Geometry, Not Geography,” *National Interest* (blog), September 17, 2024, <https://nationalinterest.org/blog/buzz/ukraines-master-stroke-kursk-offensive-about-geometry-not-geography-212768>; and Robert G. Rose, “The Kursk Offensive: How Ukraine’s Operational-Level Guerrilla Warfare Is Bringing Maneuver Back,” *Modern War Institute*, September 12, 2024, <https://mwi.westpoint.edu/the-kursk-offensive-how-ukraines-operational-level-guerrilla-warfare-is-bringing-maneuver-back/>.
- 11 Benjamin Jensen, “Ungentlemanly Robots: Israel’s Operation Rising Lion and the New Way of War,” *CSIS, Commentary*, June 13, 2025, <https://www.csis.org/analysis/ungentlemanly-robots-israels-operation-rising-lion-and-new-way-war>.
- 12 Darya Dolzikova and Matthew Savill, “Operation Rising Lion: The First 72 Hours,” *Royal United Services Institute*, June 16, 2025, <https://www.rusi.org/explore-our-research/publications/commentary/operation-rising-lion-first-72-hours>.

- 13 Thomas A. Walsh and Alexandra L. Huber, “A Symphony of Capabilities: How the Joint Warfighting Concept Guides Service Force Design,” *Joint Force Quarterly* 111 (4th Quarter 2023): 4-15, <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3568312/a-symphony-of-capabilities-how-the-joint-warfighting-concept-guides-service-for/>.
- 14 In military theory, culmination refers to the specific moment in time and space when an attacking force’s ability (i.e., combat power) no longer exceeds that of the defender either due to attrition or a breakdown in the latter’s ability to sustain operations.
- 15 As quoted in Carter Johnston, “Breaking Down the U.S. Navy’s ‘Hellscape’ in Detail,” *Naval News*, June 16, 2024, <https://www.navalnews.com/naval-news/2024/06/breaking-down-the-u-s-navys-hellscape-in-detail/>. See also Benjamin Jensen and John Paschkewitz, “Mosaic Warfare: Small and Scalable Are Beautiful,” *War on the Rocks*, December 23, 2019, <https://warontherocks.com/mosaic-warfare-small-and-scalable-are-beautiful/>; Benjamin Jensen, “Operational Art for the Replicator Initiative: Confessions of a Swarming Addict,” *War on the Rocks*, October 25, 2023, <https://warontherocks.com/operational-art-for-the-replicator-initiative-confessions-of-a-swarming-addict/>; Bryan Clark et al., *Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations* (Washington, DC: CSBA, February 11, 2020), <https://csbaonline.org/research/publications/mosaic-warfare-exploiting-artificial-intelligence-and-autonomous-systems-to-implement-decision-centric-operations/>; Benjamin Jensen, “Bringing the Swarm to Life: Roles, Missions, and Campaigns for the Replicator Initiative,” *War on the Rocks*, February 13, 2024, <https://warontherocks.com/bringing-the-swarm-to-life-roles-missions-and-campaigns-for-the-replicator-initiative/>; Kelley M. Saylor, “DOD Replicator Initiative: Background and Issues for Congress,” Congressional Research Service, IF12611, January 21, 2026, <https://www.congress.gov/crs-product/IF12611>.
- 16 Benjamin Jensen and Ian Fletcher, “Blinding First, Striking Fast: Why the Marine Corps Needs Information Groups,” *War on the Rocks*, October 13, 2025, <https://warontherocks.com/blinding-first-striking-fast-why-the-marine-corps-needs-information-groups/>.
- 17 In military theory, force closure describes the completion of deployment and integration required to generate combat power.
- 18 Lauren Kahn, “Scaling the Future: How Replicator Aims to Fast-Track U.S. Defense Capabilities,” *War on the Rocks*, September 20, 2023, <https://warontherocks.com/scaling-the-future-how-replicator-aims-to-fast-track-u-s-defense-capabilities/>; Joseph Clark, “Defense Innovation Official Says Replicator Initiative Remains On Track,” U.S. Department of Defense, January 26, 2024, <https://www.war.gov/News/News-Stories/Article/Article/3657609/defense-innovation-official-says-replicator-initiative-remains-on-track/>; and “Ukraine to Produce One Million Drones next Year, Zelenskiy Says,” *Reuters*, December 19, 2023, <https://www.reuters.com/world/europe/ukraine-produce-one-million-drones-next-year-zelenskiy-says-2023-12-19/>.
- 19 Michael C. Horowitz, “Battles of Precise Mass: Technology Is Remaking War—and America Must Adapt,” *Foreign Affairs*, October 22, 2024, <https://www.foreignaffairs.com/world/battles-precise-mass-technology-war-horowitz>.
- 20 On joint island landing campaigns, see Zhang Yuliang ed. *Science of Campaigns* (2006), *In In Their Own Words: Foreign Military Thought*. trans. Project Everest (Montgomery, AL: China Aerospace Studies Institute, 2020), [https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-12-02%20In%20Their%20Own%20Words-%20Science%20of%20Campaigns%20\(2006\).pdf?ver=hma387iK8lQcZQ1x9ktt-Q%3d%3d](https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2020-12-02%20In%20Their%20Own%20Words-%20Science%20of%20Campaigns%20(2006).pdf?ver=hma387iK8lQcZQ1x9ktt-Q%3d%3d); Andrew S. Erickson et al., *Chinese Amphibious Warfare: Prospects for a Cross-Strait Invasion*, CMSI Studies in Chinese Maritime Development Study No. 8 (Newport: U.S. Naval War College, November 8, 2024), <https://digital-commons.usnwc.edu/cmsi-studies/8>; Sugiura Yasuyuki, *The PLA’s Pursuit of Enhanced Joint Operations Capabilities* (Tokyo: National Institute for Defense Studies, Japan, 2021), https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2022_A01.

- pdf; Max Stewart, “Island Blitz: A Campaign Analysis of a Taiwan Takeover by the PLA,” Center for International Maritime Security, June 13, 2023, <https://cimsec.org/island-blitz-a-campaign-analysis-of-a-taiwan-takeover-by-the-pla/>; Joel Wuthnow, ed., et al., *Crossing the Strait: China’s Military Prepares for War with Taiwan* (Washington, DC: National Defense University Press (NDU), 2022), <https://ndupress.ndu.edu/Portals/68/Documents/Books/crossing-the-strait/crossing-the-strait.pdf>; Vermilion China, “The PLA Landing Template: The People’s Liberation Army 4 Stage Maritime Conveyor Belt (海上輸送帶),” Vermilion China, September 8, 2024, <https://www.vermilionchina.com/p/the-pla-landing-template>; Kevin McCauley, “PLA Yijiangshan Joint Amphibious Operation: Past Is Prologue,” Jamestown Foundation, China Brief 16, no. 14 (September 2016), <https://jamestown.org/pla-yijiangshan-joint-amphibious-operation-past-is-prologue/>; N. Luke Roth, “PLA Modernizing Amphibious Combined Arms Brigades For Joint Island Landing Campaign,” T2COM G2 Operational Environment Enterprise, U.S. Army Transformation and Training Command, G-2 (T2COM G2), July 22, 2025, <https://oe.t2com.army.mil/product/pla-modernizing-amphibious-combined-arms-brigades-for-joint-island-landing-campaign/>; Cristina L. Garafola, *The PLA Airborne Corps in a Joint Island Landing Campaign*, CMSI China Maritime Reports No. 19 (Newport: U.S. Naval War College, March 2022), <https://digital-commons.usnwc.edu/cmsi-maritime-reports/19>; T2COM G2, *How China Fights in Large-Scale Combat Operations*, T2COM OE Threat Assessment no. 1-1 (Austin, TX: U.S. Army Transformation and Training Command, G-2, April 30, 2025), <https://api.army.mil/e2/c/downloads/2025/05/08/1888a601/tradoc-g2-how-china-fights-in-lsco-apr-25-public.pdf>; Xu Lisheng and Wang Zhaoyang, *Research on Port Landing Operations, In In Their Own Words: Foreign Military Thought*, trans. Project Everest (Montgomery, AL: China Aerospace Studies Institute, 2022), <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2022-10-11%20ITOW%20Research%20on%20Port%20Landing%20Operations.pdf>; Benjamin Jensen, “Not So Fast: Insights from a 1944 War Plan Help Explain Why Invading Taiwan Is a Costly Gamble,” War on the Rocks, September 8, 2022, <https://warontherocks.com/not-so-fast-insights-from-a-1944-war-help-explain-why-invading-taiwan-is-a-costly-gamble/>; and Dennis J. Blasko, *The PLA Army Amphibious Force*, CMSI China Maritime Reports No. 20 (Newport: U.S. Naval War College, April 2022), <https://digital-commons.usnwc.edu/cmsi-maritime-reports/20>. On Replicator, see Jensen, “Operational Art for the Replicator Initiative”; and Jensen, “Bringing the Swarm to Life.”
- 21 Ditter, *PRC Concepts for UAV Swarms in Future Warfare*; and Emilie B. Stewart, *Survey of PRC Drone Swarm Inventions* (Montgomery, AL: China Aerospace Studies Institute, October 2023), <https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2023-10-09%20Survey%20of%20PRC%20Drone%20Swarm%20Inventions.pdf>.
 - 22 Alistair MacDonald, “AI-Powered Drone Swarms Have Now Entered the Battlefield,” *Wall Street Journal*, September 2, 2025, <https://www.wsj.com/world/ai-powered-drone-swarms-have-now-entered-the-battlefield-2cab0f05>; and Patrick Tucker, “This Ukrainian Startup Has Re-invented Drone Swarming,” *Defense One*, September 15, 2025, <https://www.defenseone.com/business/2025/09/ukrainian-startup-has-re-invented-drone-swarmling/408099/>.
 - 23 Pettyjohn, *Evolution Not Revolution*.
 - 24 John Arquilla and David Ronfeldt, *Swarming and the Future of Conflict* (Santa Monica, CA: RAND Corporation, 2000), vii, https://www.rand.org/pubs/documented_briefings/DB311.html.
 - 25 In military theory, the horns of a dilemma is a maneuver concept that refers to a tactical or strategic situation where friendly actions force an enemy commander to choose between two or more equally undesirable, dangerous, or unacceptable alternatives.
 - 26 On the concept of offsets, see Robert Martinage, *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability* (Washington, DC: CSBA, 2014), <https://csba-online.org/research/publications/toward-a-new-offset-strategy-exploiting-u-s-long-term-advantages-to-restore>.

- 27 A. J. Bacevich, *The Pentomic Era: The U.S. Army between Korea and Vietnam* (Washington, DC: NDU, 1986), <https://apps.dtic.mil/sti/pdfs/ADA956178.pdf>.
- 28 Gian Gentile et al., *A History of the Third Offset, 2014-2018*, RR-A454-1 (Santa Monica, CA: RAND Corporation, 2021), <https://doi.org/10.7249/RR-A454-1>.
- 29 C. E. Callwell, Col. *Small Wars: Their Principles and Practice* (London: Wyman and Sons, 1905), 219.
- 30 George Bruce Malleson, *Ambushes and Surprises* (London: W. H. Allen & Co., 1885), 38.
- 31 *Ibid.*, 165.
- 32 U.S. Army Training and Doctrine Command (U.S. Army TRADOC), *TRADOC Pamphlet 525-5, Force XXI Operations* (Fort Monroe, VA: U.S. Army Training and Doctrine Command, August 1994), 2-9, <https://apps.dtic.mil/sti/tr/pdf/ADA314276.pdf>.
- 33 U.S. Army TRADOC, *TRADOC Pamphlet 525-5*, 2-9.
- 34 Anthony Dekker, *A Taxonomy of Network Centric Warfare Architectures* (Canberra, Australia: Defence Science & Technology Organisation, 2008), 6, <https://apps.dtic.mil/sti/tr/pdf/ADA488254.pdf>, emphasis in original.
- 35 Jensen and Paschkewitz, “Mosaic Warfare.”
- 36 Dekker, *A Taxonomy of Network Centric Warfare Architectures*, 7.
- 37 Jules Hurst, “Robotic Swarms in Offensive Maneuver,” *Joint Force Quarterly* 87 (4th Quarter 2017): 105-11, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-87/jfq-87_105-111_Hurst.pdf.
- 38 Sean J. A. Edwards, *Swarming on the Battlefield: Past, Present, and Future* (Santa Monica, CA: RAND Corporation, 2000), xi, https://www.rand.org/pubs/monograph_reports/MR1100.html.
- 39 Edwards, *Swarming on the Battlefield*, xii. Cases that matched this criteria in the RAND study included: Battle of Alexandria Eschate (329-27 BCE), Battle of Carrhae (53 BCE), Battle of Manzikert (1071 AD), Battle of Dorylaeum (1097 AD), Battle of Liegnitz (1241 AD), St. Clair’s Defeat (1791 AD), Ulm Campaign (1805 AD), Battle of Majuba Hill (1881 AD), Battle of the Atlantic (1939-45 AD), and Battle of the Black Sea (1993 AD). Case selection criteria included selecting on combinations of opposing-force types, scale, and spectrum of war, Edwards, *Swarming on the Battlefield*, xii. Of note, in a later (2005) dissertation expanding the findings, the same author differentiates between linear and non-linear cases, selecting to confine irregular adversaries into a non-linear section. See Sean J. A. Edwards, *Swarming and the Future of Warfare* (Santa Monica, CA: RAND Corporation, May 2005), https://www.rand.org/pubs/rgs_dissertations/RGSD189.html.
- 40 Avi Kober, “The Rise and Fall of Israeli Operational Art, 1948-2008” in *The Evolution of Operational Art: From Napoleon to the Present*, John Andreas Olsen and Martin van Creveld eds. (Oxford: Oxford University Press, 2010), 166-94, <https://doi.org/10.1093/acprof:oso/9780199599486.003.0007>.
- 41 For accounts of the conflict, see Andrew Exum, *Hizballah at War: A Military Assessment*, Policy Focus no. 63 (Washington, DC: Washington Institute for Near East Policy, December 2006), <https://www.washingtoninstitute.org/policy-analysis/hizballah-war-military-assessment>; Anthony H. Cordesman et al., *Lessons of the 2006 Israeli-Hezbollah War*, Significant Issues Vol. 4, no. 4 (Washington, DC: CSIS 2007), <https://www.csis.org/analysis/lessons-2006-israeli-hezbollah-war>; and Matt M. Matthews, *We Were Caught Unprepared: The 2006 Hezbollah-Israeli War*, The Long War Series, Occasional Paper no. 26 (Fort Leavenworth, KS: U.S. Army Combined Arms Center, Combat Studies Institute Press, 2008), <https://www.armyupress.army.mil/Portals/7/combat-studies-institute/csi-books/we-were-caught-unprepared.pdf>.

- 42 Jonathan M. Jeschke and Ralph Tollrian, "Prey Swarming: Which Predators Become Confused and Why?," *Animal Behaviour* 74, issue 3 (2007): 387-93, <https://doi.org/10.1016/j.anbehav.2006.08.020>.
- 43 On the use of military history and seminal texts to define war as a non-linear system, see Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no. 3 (1992): 59-90, <https://clausewitzstudies.org/item/Beyerchen-ClausewitzNonlinearity.pdf>; and Derek M. C. Yuen, "Deciphering Sun Tzu," *Comparative Strategy* 27, no. 2 (April 2008): 183-200, <https://doi.org/10.1080/01495930801944727>.
- 44 Andrew Ilachinski, *Land Warfare and Complexity, Part II: An Assessment of the Applicability of Nonlinear Dynamic and Complex Systems Theory to the Study of Land Warfare* (Alexandria, VA: CNA, July 1996), 3, <https://apps.dtic.mil/sti/pdfs/ADA362621.pdf>.
- 45 David E. Hiebeler, "The Swarm Simulation System and Individual-Based Modeling," Santa Fe Institute, SFI Working Paper 1994-11-065, September 12, 1994, <https://sfi-edu.s3.amazonaws.com/sfi-edu/production/uploads/sfi-com/dev/uploads/filer/0f/c0/0fc0ee6f-a7ed-4996-830b-af0634d04e69/94-11-065.pdf>.
- 46 Jensen and Fletcher, "Blinding First, Striking Fast."
- 47 Frans P. B. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Abingdon, UK: Routledge, 2007), 237.
- 48 "Countering Russia's Unjammable Drones," Nordic Defence Review, accessed May 28, 2026, <https://nordicdefencereview.com/countering-russias-unjammable-drones/>; and "Can Traditional Radar Monitor and Track Drones?," Autelpilot (blog), September 27, 2023, <https://www.autelpilot.com/blogs/skyfend/can-traditional-radar-monitor-and-track-drones>.
- 49 Cyril Barabaltchouk, "Russia Fields Jam-Resistant 50km Fiber-Optic Drones—Ukraine to Deploy Interceptors and Cable Defenses," UNITED24 Media, November 17, 2025, <https://united24media.com/latest-news/russia-fields-jam-resistant-50km-fiber-optic-drones-ukraine-to-deploy-interceptors-and-cable-defenses-13490>.
- 50 Maximilian K. Bremer and Kelly A. Grieco, "The Air Littoral: Another Look," *Parameters* 51, no. 4 (2021): 67-80, <https://doi.org/10.55540/0031-1723.3092>; Kelly A. Grieco and Maximilian K. Bremer, "Contesting the Air Littoral," *Æther: A Journal of Strategic Airpower & Spacepower* 3, no. 3 (2024): 10-24, https://www.airuniversity.af.edu/Portals/10/ÆtherJournal/Journals/Volume-3_Number-3/Grieco_and_Bremer.pdf; and Jim E. Rainey and James K. Greer, "Land Warfare and the Air-Ground Littoral," *Army Aviation Magazine*, 14-17, December 21, 2023, <https://vertex.aal.mil/assets/files/vertex-agl-article.pdf>.
- 51 Critics of the air littoral assert this space is already accounted for in airspace control measures, see U.S. Air Force, *Airspace Control*, Air Force Doctrine Publication 3-52 (Montgomery, AL: Curtis E. LeMay Center for Doctrine Development and Education, September 2025), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-52/3-52-AFDP-AIRSPACE-CONTROL.pdf.
- 52 Maximilian K. Bremer and Kelly A. Grieco, "Air Denial: The Dangerous Illusion of Decisive Air Superiority," Atlantic Council, August 30, 2022, <https://www.atlanticcouncil.org/content-series/airpower-after-ukraine/air-denial-the-dangerous-illusion-of-decisive-air-superiority/>.
- 53 General Atomics Aeronautical (GA-ASI), "GA-ASI Demonstrates Release of A2LE from MQ-20 Avenger UAS," press release, February 1, 2024, <https://www.ga-asi.com/ga-asi-demonstrates-release-of-a2le-from-mq-20-avenger-uas>.
- 54 Jen Judson, "General Atomics Demos 3-D Printed Air-Launched Effects Vehicle," C4ISRNet, February 1, 2024, <https://www.c4isrnet.com/battlefield-tech/2024/02/01/general-atomics-demos-3-d-printed-air-launched-effects-vehicle/>; and GA-ASI, "GA-ASI Demonstrates Release of A2LE from MQ-20 Avenger UAS."

- 55 GA-ASI, “GA-ASI’s Eaglet Takes Its First Flight,” press release, January 31, 2023, <https://www.ga.com/ga-asi-s-eaglet-takes-its-first-flight>; and Stefano D’Urso, “General Atomics Tests New Eaglet Air Launched Effect,” *The Aviationist*, February 17, 2023, <https://theaviationist.com/2023/02/17/general-atomics-tests-new-eaglet-air-launched-effect/>.
- 56 GA-ASI, “GA-ASI’s Eaglet Takes Its First Flight.”
- 57 “Gray Eagle 25M: Standoff Survivability with Stand-In Capability,” datasheet P07481 (Poway, CA: General Atomics Aeronautical Systems, September 19, 2022), https://www.ga-asi.com/remotely-piloted-aircraft/pdf/2209_Gray_Eagle_25M_Datasheet_P07481_29SEPT22.pdf; and Judson, “General Atomics Demos 3-D Printed Air-Launched Effects Vehicle.”
- 58 “Gray Eagle,” General Atomics Aeronautical Systems, Inc., accessed September 4, 2026, <https://ga-asi.com/remotely-piloted-aircraft/gray-eagle>.
- 59 Howard Altman, “Eaglet Air-Launched Drone Aims to Help Its Mothership Survive in Army Tests,” *The War Zone*, May 19, 2022, <https://www.twz.com/eaglet-air-launched-drone-aims-to-help-its-mothership-survive-in-army-tests>.
- 60 Stefano D’Urso, “General Atomics Provides Detailed Look at Sparrowhawk Air-Launched and Air-Retrieveable Small UAS,” *The Aviationist*, August 9, 2021, <https://theaviationist.com/2021/08/09/sparrowhawk/>; and GA-ASI, “Small Unmanned Aerial Systems and Launched Effects,” accessed March 10, 2026, <https://www.ga-asi.com/remotely-piloted-aircraft/small-uas-and-launched-effects>.
- 61 “GA-ASI Conducts Sparrowhawk sUAS Flight Tests,” GA-ASI, September 25, 2020, <https://www.ga-asi.com/ga-asi-conducts-sparrowhawk-suas-flight-tests?>.
- 62 “GA-ASI Advances Aerial Recovery for SUAS and ALE,” GA-ASI, October 10, 2023, <https://www.ga-asi.com/ga-asi-advances-aerial-recovery-for-suas-and-ale>.
- 63 Howard Altman, “Eaglet Air-Launched Drone Aims to Help Its Mothership Survive in Army Tests,” *The War Zone (TWZ)*, May 19, 2022, <https://www.twz.com/eaglet-air-launched-drone-aims-to-help-its-mothership-survive-in-army-tests>.
- 64 RTX, “RTX’s Raytheon’s Non-Kinetic Coyote Variant Defeats Multiple Drone Swarms,” news release, February 11, 2026, <https://raytheon.mediaroom.com/2026-02-11-RTXs-Raytheons-non-kinetic-Coyote-variant-defeats-multiple-drone-swarms>.
- 65 Evan Lerouvillos, “U.S. Army Tests Reusable Coyote 3NK Interceptor to Counter Drone Swarms Without Missiles,” *Global Defense News*, February 12, 2026, <https://www.armyrecognition.com/news/aerospace-news/2026/u-s-army-tests-reusable-coyote-3nk-interceptor-to-counter-drone-swarms-without-missiles>.
- 66 “Coyote C-UAS,” Raytheon, RTX, accessed October 9, 2026, <https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/coyote>; and “RTX’s Raytheon’s Non-Kinetic Coyote Variant Defeats Multiple Drone Swarms,” RTX, February 11, 2026, <https://www.rtx.com/news/news-center/2026/02/11/rtxs-raytheons-non-kinetic-coyote-variant-defeats-multiple-drone-swarms>.
- 67 U.S. Army, “U.S. Army Taps Three Companies for Cutting-Edge Launched Effects Demonstration,” press release, March 27, 2025, https://www.army.mil/article/284204/u_s_army_taps_three_companies_for_cutting_edge_launched_effects_demonstration; and Matthew Ryan, “Groundbreaking Launched Effects Demonstration Marks Key Step in U.S. Army Modernization Strategy,” U.S. Army, October 2, 2025, https://www.army.mil/article/288878/groundbreaking_launched_effects_demonstration_marks_key_step_in_u_s_army_modernization_strategy.
- 68 Dan Schere, “Army Updates Requirements Document for Launched Effects,” *Inside Defense*, July 19, 2024, <https://insidedefense.com/share/221645>.

- 69 “Altius,” Anduril, accessed March 10, 2026, <https://www.anduril.com/altius>; and Raghavi Joshi, “ALTIUS-600 Small Unmanned Aircraft System,” Airforce Technology, April 28, 2021, <https://www.air-force-technology.com/projects/altius-600-small-unmanned-aircraft-system/>.
- 70 Joshi, “ALTIUS-600 Small Unmanned Aircraft System”; and Matthew Cox, “Air Force Buying \$50M in Small Drones to Support Special Ops,” *Air & Space Forces Magazine*, November 19, 2025, <https://www.airandspaceforces.com/air-force-anduril-altius-drones-afsoc-mq-9/>.
- 71 Matthew Beinart, “Army Selects AEVEX’s Atlas, Anduril’s Altius 600 For Launched Effects-Short Range Fielding,” *Defense Daily*, October 13, 2025, <https://www.defensedaily.com/army-selects-aevex-atlas-andurils-altius-600-for-launched-effects-short-range-fielding/army/>.
- 72 “Altius,” Anduril.
- 73 “U.S. Army Selects AEVEX Atlas for Initial Launched Effects Fielding,” *BusinessWire*, October 28, 2025, <https://www.businesswire.com/news/home/20251028462586/en/U.S.-Army-Selects-AEVEX-Atlas-for-Initial-Launched-Effects-Fielding>; and “U.S. Army Selects AEVEX Atlas for Initial Launched Effects Fielding,” *Inside Unmanned Systems*, October 28, 2025, <https://insideunmannedsystems.com/u-s-army-selects-aevex-atlas-for-initial-launched-effects-fielding/>.
- 74 “Atlas,” AEVEX Aerospace, accessed March 10, 2026, <https://aevex.com/unmanned-systems/precision-strike-systems/atlas/>.
- 75 The Atlas provides 70+ minutes of endurance, 70+ nautical miles (~130 km) of range, a 65 kt cruise (up to 87 kt dash), and a 7.5 lb kinetic or ISR payload, packaged in a 36.5 lb man-portable airframe. “ATLAS,” AEVEX, accessed May 28, 2026, https://aevex.com/wp-content/uploads/2025/10/Atlas-Card-10.31.25_1a.pdf; and “How AEVEX Aerospace’s Atlas Group II Drone Could Redefine US Army’s Short-Range Launched Effects,” *Global Defense News*, April 29, 2025, <https://www.armyrecognition.com/news/aerospace-news/2025/how-aevex-aerospaces-atlas-group-ii-drone-could-redefine-us-armys-short-range-launched-effects>.
- 76 “U.S. Army Selects AEVEX Atlas for Initial Launched Effects Fielding,” *Inside Unmanned Systems*.
- 77 Brian Everstine, “U.S. Army Picks AEVEX Atlas For Launched Effect-Short Range,” *Aviation Week*, October 28, 2025, <https://aviationweek.com/defense/aircraft-propulsion/us-army-picks-aevex-atlas-launched-effect-short-range>.
- 78 Judson, “General Atomics Demos 3-D Printed Air-Launched Effects Vehicle.”
- 79 Garrett Reim, “U.S. Army Funds Project To 3D Print Drone Fuselage from Composites,” *Aviation Week*, June 13, 2025, <https://aviationweek.com/defense/aircraft-propulsion/us-army-funds-project-3d-print-drone-fuselage-composites>.
- 80 Jay Menon, “US Air Force Backs Beehive’s Frenzy Engine to Power Swarm Drones,” *Aerospace Global News*, April 10, 2026, <https://aerospaceglobalnews.com/news/us-air-force-beehive-industries-frenzy-engine-drone/>.
- 81 Lily-Swann, “Built for the Battlefield: 3D-Printed Drones Move to the Front Lines,” *3Dnatives*, April 9, 2026, <https://www.3dnatives.com/en/3d-printed-drones-battlefield-09042026/>.
- 82 Horowitz, “Battles of Precise Mass.”
- 83 Brandi Vincent, “DOD Touts ‘Successful Transition’ for Replicator Initiative—but Questions Linger,” *DefenseScoop*, September 3, 2025, <https://defensescoop.com/2025/09/03/dod-replicator-drone-tech-transition-fielding-questions-linger/>; Sayler, *DOD Replicator Initiative*; Ryan, “Groundbreaking Launched Effects Demonstration”; and U.S. Navy, *U.S. Navy Fighting Instructions* (Arlington, VA: U.S. Navy, Febru-

- ary 2026), <https://media.defense.gov/2026/Feb/06/2003871752/-1/-1/1/CNO%20FIGHTING%20INSTRUCTIONS.PDF/CNO%20FIGHTING%20INSTRUCTIONS.PDF>.
- 84 Michael Scanlon, “US Air Force Turns to Cheaper Cruise Missiles It Can Buy by the Thousands,” *Military Times*, July 15, 2026, <https://www.militarytimes.com/industry/techwatch/2026/07/15/us-air-force-turns-to-cheaper-cruise-missiles-it-can-buy-by-the-thousand/>.
- 85 Theresa Maher, “Pentagon Seeking Scalable, Affordable Long-Range Precision Strike Systems to Complement High-Cost Munitions,” *Inside Defense*, July 22, 2026, <https://insidedefense.com/daily-news/pentagon-seeking-scalable-affordable-long-range-precision-strike-systems-complement-high>; Bill Daly and Lawrence Heyworth IV, “Containerized Payloads: Modular Lethality,” U.S. Naval Institute, *Proceedings* 151, no. 6 (June 2025), <https://www.usni.org/magazines/proceedings/2025/june/containerized-payloads-modular-lethality>.
- 86 Jensen, “Operational Art in the Age of Battle Networks.”
- 87 Joint Staff, *Deployment and Redeployment Operations*, Joint Publication 3-35 (Washington, DC: Joint Chiefs of Staff, January 2018), https://www.bits.de/NRANEU/others/jp-doctrine/jp3_35%282018%29.pdf.
- 88 See Joint Staff, *Joint Intelligence Preparation of the Operational Environment*, Joint Publication 2-01.3 (Washington, DC: Joint Chiefs of Staff, May 2014), <https://irp.fas.org/doddir/dod/jp2-01-3.pdf>.
- 89 Joint Staff, *Joint Electromagnetic Spectrum Operations*, CJCSM 3320.01D (Arlington, VA: Joint Chiefs of Staff, January 2025), <https://www.jcs.mil/Portals/36/Documents/Library/Manuals/CJCSM%203320.01D.pdf>; *Electromagnetic Spectrum Operations*, Air Force Doctrine Publication no. 3-85 (Arlington, VA: U.S. Air Force, December 2023), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-85/AFDP%203-85%20Electromagnetic%20Spectrum%20Ops.pdf; and U.S. Army Training and Doctrine Command, *The U.S. Army Concept for Cyberspace and Electronic Warfare Operations: 2025-2040*, TRADOC Pamphlet no. 525-8-6 (Fort Eustis, VA: U.S. Army Training and Doctrine Command, January 2018), <https://admin-pubs.tradoc.army.mil/pamphlets/TP525-8-6.pdf>.
- 90 U.S. Department of the Army, *Engineer Reconnaissance*, ATP 3-34.81 / MCWP 3-17.4 (Arlington, VA: U.S. Department of the Army, March 2016), <https://www.marines.mil/Portals/1/Publications/MCWP%203-17.4.pdf>.
- 91 Joint Staff, *Special Operations*, JP 3-05 (Arlington, VA: Joint Chiefs of Staff, 2020); legal authority is Title 10 section 127f, see: 10 U.S. Code § 127f—Expenditure of Funds for Clandestine Activities That Support Operational Preparation of the Environment and Non-Conventional Assisted Recovery Capabilities, 10 U.S. Code § 127f, accessed May 12, 2026, <https://www.law.cornell.edu/uscode/text/10/127f>.
- 92 Joint Staff, *Special Operations*, JP 3-05.
- 93 U.S. Special Forces Command (USSOCOM), *Special Forces Operations*, Field Manual FM 3-18 (Arlington, VA: Department of the Army, May 2014), <https://www.recoons.org/files/Doctrine%20and%20Training/Field%20Manual/FM3-18-SpecialForcesOperations.pdf>.
- 94 Joint Staff, *The Defense Transportation System*, Joint Publication 4-01 (Arlington, VA: Joint Chiefs of Staff, June 2013), <https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/DefenseTransportationSystem.pdf>; and Secretary of the Air Force, *Department of the Air Force Manual (DAFMAN) 21-201, Maintenance: Munitions Management* (Washington, DC: Department of the Air Force, October 2024), https://static.e-publishing.af.mil/production/1/af_a4/publication/dafman21-201/dafman21-201.pdf.
- 95 Chairman of the Joint Chiefs of Staff, *Military Deception*, Joint Publication 3-13.4 (Arlington, VA: Joint Chiefs of Staff, January 2012), https://jfc.ndu.edu/portals/72/documents/jc2ios/additional_reading/1c3-jp_3-13-4_mildec.pdf.

- 96 Joint Staff, *Military Deception*, JP 3-13.4 (Arlington, VA: Joint Chiefs of Staff, 2012), https://jpsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf.
- 97 Benjamin Jensen, "Fighting for Information: A Theory of Tactics for the Next Army," CSIS, Commentary, June 11, 2025, <https://www.csis.org/analysis/fighting-information-theory-tactics-next-army>.
- 98 Evans, "Ukraine's Kursk Incursion."
- 99 Mick Ryan, "ANALYSIS: The Battle of Kursk 2024," Lowy Institute, August 8, 2024, <https://www.lowyinstitute.org/external-publications/analysis-battle-kursk-2024>.
- 100 Pavel Luzin, "Lessons of Kursk Incursion for Taiwan," Prospect Foundation, October 1, 2024, <https://www.pf.org.tw/tw/pfch/13-10942.html>.
- 101 Mykola Bielieskov, "Ukraine's Kursk Offensive Proves Surprise Is Still Possible in Modern War," Atlantic Council, *UkraineAlert (blog)*, August 13, 2024, <https://www.atlanticcouncil.org/blogs/ukrainealert/ukraines-kursk-offensive-proves-surprise-is-still-possible-in-modern-war/>.
- 102 Dan Sabbagh, "Kursk Incursion: How Ukraine Turned the Tables and Struck Back at Russia," *The Guardian*, August 16, 2024, <https://www.theguardian.com/world/article/2024/aug/16/kursk-incursion-how-ukraine-turned-the-tables-and-struck-back-at-russia>.
- 103 Vadim Kushnikov, "SOF Operators Conducted a Raid behind Enemy Lines in the Kursk Oblast," *MilitarNYI*, November 10, 2024, <https://militarnyi.com/en/news/sof-operators-conducted-a-raid-behind-enemy-lines-in-the-kursk-oblast/>.
- 104 Ben Barry, "Ukraine's Kursk Offensive: Big Stakes, Big Risks for Both Sides," International Institute for Strategic Studies, *Military Balance (blog)*, August 22, 2024, <https://www.iiss.org/online-analysis/military-balance/2024/08/ukraines-kursk-offensive-big-stakes-big-risks-for-both-sides/>.
- 105 Asami Terajima, "The Rise and Fall of Ukraine's Kursk Gambit," *Kyiv Independent*, April 1, 2025, <https://kyivindependent.com/the-rise-and-fall-of-ukraines-kursk-gambit/>.
- 106 Ryan, "ANALYSIS: The Battle of Kursk 2024."
- 107 Dorsel Boyer and ISC Robert K. Becker, "How Ukraine Overcame the Transparent Battlefield to Achieve Operational Surprise in Kursk," T2COM G2, September 19, 2024, <https://oe.t2com.army.mil/product/how-ukraine-overcame-the-transparent-battlefield-to-achieve-operational-surprise-in-kursk/>.
- 108 Stefan Korshak, "Five Things Worth Knowing About Ukraine's Kursk Offensive in Russia," *Kyiv Post*, August 16, 2024, <https://www.kyivpost.com/post/37451>.
- 109 Jensen, "Fighting for Information."
- 110 Department of the Army, *Offense and Defense*, ADP 3-90 (Arlington, VA: Department of the Army, 2019), 31, https://irp.fas.org/doddir/army/adp3_90.pdf.
- 111 Department of the Army, *Operations*, FM 3-0 (Arlington, VA: Department of the Army, 2022), 3-13, https://soldat-und-technik.de/wp-content/uploads/2022/10/ARN36290-FM_3-0.pdf.
- 112 Edwards, *Swarming and the Future of Warfare*.
- 113 Marine Corps, *Warfighting*, MCDP 1 (Arlington, VA: Department of the Navy, June 1997), <https://www.marines.mil/portals/1/publications/mcdp%201%20warfighting.pdf>.
- 114 Department of the Army, *Offense and Defense*, ADP 3-90, 5-3.
- 115 Department of the Army, *Operations*, FM 3-0, 1-19

- 116 Kristin Lechowicz, “Ukrainian Ambush Overwhelms Russian Mechanized Column Using Hunter-Killer Team Tactics,” T2COM G2, August 22, 2025, <https://oe.t2com.army.mil/product/ukrainian-ambush-overwhelms-russian-mechanized-column-using-hunter-killer-team-tactics/>.
- 117 Kateryna Denisova, “First Ukrainian Troops Crossed into Kursk Oblast 2 Days before Incursion, Commander Says,” *Kyiv Independent*, October 14, 2024, <https://kyivindependent.com/80-brigade-kursk/>.
- 118 Guy Faulconbridge, “Russia Fighting Intense Battles against Major Ukrainian Incursion,” Reuters, August 10, 2024, <https://www.reuters.com/world/europe/russia-imposes-security-regime-three-border-regions-after-major-ukrainian-attack-2024-08-10/>; Guy Faulconbridge, “Russia Imposes Security Regime on Three Border Regions after Major Ukrainian Attack,” WHBL, August 10, 2024, <https://whbl.com/2024/08/10/russia-imposes-security-regime-on-three-border-regions-after-major-ukrainian-attack/>; and Dan Sabbagh and Pjotr Sauer, “Ukraine Justifies Kursk Attack in First Acknowledgment of Incursion into Russia,” *The Guardian*, August 8, 2024, <https://www.theguardian.com/world/article/2024/aug/08/ukraine-justifies-attack-on-kursk-in-first-acknowledgement-of-its-russian-incursion>.
- 119 Evans, “Ukraine’s Kursk Incursion.”
- 120 Faulconbridge, “Russia Fighting Intense Battles against Major Ukrainian Incursion.”
- 121 Ryan, “ANALYSIS: The Battle of Kursk 2024.”
- 122 SOFX Staff Writer, “Ukrainian Tactics in Kursk: Electronic Warfare, Drones, and the Russian Response,” SOFX, August 12, 2024, <https://www.sofx.com/ukrainian-tactics-in-kursk-electronic-warfare-drones-and-the-russian-response/>.
- 123 Boyer and Becker, “How Ukraine Overcame the Transparent Battlefield to Achieve Operational Surprise in Kursk.”
- 124 Jeremy Dirac, “Ukraine Hacks ATMs Across Russia in Ongoing Massive Cyberattack,” *Kyiv Post*, July 27, 2024, <https://www.kyivpost.com/post/36471>; and Kateryna Zakharchenko, “HUR Hackers Shut Down Russian Banks and Internet Providers,” *Kyiv Post*, July 24, 2024, <https://www.kyivpost.com/post/36296>.
- 125 Nate Ostiller, “Over 220 Russian Soldiers Surrender through ‘I Want to Live’ Hotline,” *Kyiv Independent*, January 4, 2024, <https://kyivindependent.com/more-than-220-russian-soldiers-surrendered-through-i-want-to-live-hotline/>.
- 126 Howard Altman, “Ukrainian Forces Make Major Gains Inside Russia on Day Three of Kursk Invasion (Updated),” TWZ, August 8, 2024, <https://www.twz.com/air/ukrainian-forces-make-major-gains-inside-russia-on-day-three-of-kursk-invasion>.
- 127 “Ukrainian FPV Drones Target Russian Pontoon Crossings in Kursk (Video),” Defense Express, August 20, 2024, https://en.defence-ua.com/weapon_and_tech/ukrainian_fpv_drones_target_russian_pontoon_crossings_in_kursk_video-11583.html.
- 128 Lechowicz, “Ukrainian Ambush Overwhelms Russian Mechanized Column Using Hunter-Killer Team Tactics.”
- 129 Department of the Army, *Operations*, FM 3-0 (Arlington, VA: Department of the Army, 2022), 6-25.
- 130 Department of the Army, *Offense and Defense*, ADP 3-90 (Arlington, VA: Department of the Army, 2019), 3-10.
- 131 Ibid., 5-16.
- 132 Department of the Army, *Operations*, FM 3-0, 8-9.
- 133 Barry, “Ukraine’s Kursk Offensive.”

- 134 Ryan, "ANALYSIS: The Battle of Kursk 2024."
- 135 SOFX Staff Writer, "Ukrainian Tactics in Kursk."
- 136 Hafsa Khalil, "Ukraine Incursion Destroys Key Russian Bridge in Kursk Region," BBC, August 16, 2024, <https://www.bbc.com/news/articles/c628gk68p3po>.
- 137 David Axe, "Ukraine Is Blowing Up Bridges in Kursk as Fast as Russia Builds Them," Forbes, August 21, 2024, <https://www.forbes.com/sites/davidaxe/2024/08/21/ukraine-is-blowing-up-bridges-in-kursk-as-fast-as-russia-can-build-them/>.
- 138 Department of the Air Force, *Counterair Operations*, Air Force Doctrine Publication 3-01 (Arlington, VA: Department of the Air Force, June 2023), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-01/3-01-AFDP-COUNTERAIR.pdf, formerly Joint Staff, *Countering Air and Missile Threats* JP 3-01 (Arlington, VA: Joint Chiefs of Staff, April 2023); Joint Staff, *JTTP Joint Tactics for Joint Suppression of Enemy Air Defenses* (J-SEAD), JP 3-01.4 (Arlington, VA: Joint Chiefs of Staff, July 1995), [https://www.bits.de/NRANEU/others/jp-doctrine/jp3_01_4\(95\).pdf](https://www.bits.de/NRANEU/others/jp-doctrine/jp3_01_4(95).pdf).
- 139 Department of the Air Force, *Air Force Doctrine Publication 3-01: Counterair Operations*, AFDP 3-01 (Arlington, VA: Department of the Air Force, June 2023), https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-01/3-01-AFDP-COUNTERAIR.pdf.
- 140 Marine Corps, *Antiair Warfare*, MCTP 3-20C (formerly MCWP 3-22) (Arlington, VA: Department of the Navy, April 2018), <https://www.marines.mil/portals/1/Publications/MCTP%203-20C%20GN.pdf?ver=2019-01-31-114859-677>.
- 141 Jensen et al., *Information in War*.
- 142 Ibid.
- 143 "NATO Integrated Air and Missile Defence," NATO, updated February 13, 2025, <https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-integrated-air-and-missile-defence>.
- 144 Howard Altman and Tyler Rogoway, "Ukraine's Acoustic Drone Detection Network Eyed by U.S. as Low-Cost Air Defense Option," TWZ, July 24, 2024, <https://www.twz.com/air/ukraines-acoustic-drone-detection-network-eyed-by-u-s-as-low-cost-air-defense-option>; Sebastian Clapp, "Eastern Flank Watch and European Drone Wall," European Parliamentary Research Service (EPRS), October 2025, [https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777962/EPRS_ATA\(2025\)777962_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2025/777962/EPRS_ATA(2025)777962_EN.pdf); Andrew Gray and Lili Bayer, "European Drone Wall, Other 'Flagship' Defence Projects at Risk in EU Power Struggle," Reuters, December 15, 2025, <https://www.reuters.com/business/aerospace-defense/european-drone-wall-other-flagship-defence-projects-risk-eu-power-struggle-2025-12-15/>; and Secretary of Defense, "Establishment of Joint Interagency Task Force 401," Memorandum, Department of Defense, August 27, 2025, <https://media.defense.gov/2025/Aug/28/2003790021/-1/-1/0/ESTABLISHMENT-OF-JOINT-INTER-AGENCY-TASK-FORCE-401.PDF>.
- 145 A cosine wave is a mathematical graph representing the cosine function. Here, it denotes a smooth, continuous, periodic oscillation.
- 146 Stacie Pettyjohn and Molly Campbell, *Countering the Swarm: Protecting the Joint Force in the Drone Age* (Washington, DC: CNAS, September 2025), <https://www.cnas.org/publications/reports/countering-the-swarm>.
- 147 For Iskander-M, Iskander-K, Kalibr, S-400, Pantsir-S, Bastion-P, and Bal, see Robert Dalsjö, Christofer Berglund, and Michael Jonsson, *Bursting the Bubble? Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications*, FOI-R--4651--SE (Stockholm: Swedish Defence Research Agency, March 2019), <https://www.foi.se/rest-api/report/FOI-R--4651--SE>. For S-400, Bastion-P, and Krasukha-4,

- see Eric Rosenbach et al., *Russian Threats to NATO's Eastern Flank: Scenarios, Strategy, and Policy for European Security* (Cambridge, MA: Belfer Center for Science and International Affairs, February 2026), https://www.belfercenter.org/sites/default/files/2026-02/Belfer_Russian%20Threats_3.1.pdf. For Iskander-M, S-400, Bastion-P, Bal, Krasukha, Murmansk-BN, Su-24M, Su-27, Su-30SM, and the Steregushchiy-, Karakurt-, and Buyan-class corvettes, see Konrad Muzyka, Russian Forces in the Western Military District, CNA Occasional Paper IOP-2020-U-028759-1Rev (Arlington, VA: CNA, June 2021), 42-51, <https://www.cna.org/reports/2021/06/Russian-Forces-in-the-Western-Military-District.pdf>. For S-300V, see "S-300," Missile Threat, CSIS, last modified July 6, 2021, <https://missilethreat.csis.org/defsys/s-300/>. For Su-27SM3, see Iwona Wiśniewska et al., *Kaliningrad Oblast 2016: The Society, Economy and Army*, OSW Report (Warsaw: Centre for Eastern Studies, December 2016), 30, https://www.osw.waw.pl/sites/default/files/raport_in_the_kaliningrad_net.pdf. For Su-30SM2, see "Russia to Send Ten Modernised Su-30SM2 Fighters to Kaliningrad: Optimised for Bombing Central Europe," Military Watch Magazine, <https://militarywatchmagazine.com/article/russia-ten-su30sm2-bombing-central-europe>. For Tor-M2, see "Baltic Fleet Ships Conduct Exercises to Repel 'Enemy' Air Attacks," TASS, <https://tass.com/defense/2016235>. For system ranges, see "OE Data Integration Network (ODIN)," U.S. Army TRADOC, <https://odin.tradoc.army.mil>.
- 148 "S-400 Triumph," *Missile Threat*, CSIS Missile Defense Project, updated July 6, 2021, <https://missilethreat.csis.org/defsys/s-400-triumph/>; Krishna Duddilla, "S-400 Triumph Air Defence Missile System," *Army Technology*, February 3, 2020, <https://www.army-technology.com/projects/s-400-triumph-air-defence-missile-system/>; and Jayakrishnan N. Nair, "'S-400 Triumph'—Big Boost to India's Air Defence Infrastructure (Part-2 of 3)," *Defence Research and Studies*, October 16, 2020, <https://dras.in/s-400-triumph-big-boost-to-indias-air-defence-infrastructure-part-2-of-3/>.
- 149 Justin Bronk, *Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options*, Occasional Paper January 2020 (London: Royal United Services Institute, January 2020), 10, https://static.rusi.org/20191118_iads_bronk_web_final.pdf; and "S-400 Triumph Air Defence Missile System," *Army Technology*, February 3, 2020, <https://www.army-technology.com/projects/s-400-triumph-air-defence-missile-system/>.
- 150 Dalsjö, Berglund, and Jonsson, *Bursting the Bubble?*; "Pantsir S-1," *Missile Threat*, CSIS Missile Defense Project, updated July 6, 2021, <https://missilethreat.csis.org/defsys/pantsir-s-1/>; "S-400 Triumph Air Defence Missile System," *Army Technology*; and Justin Bronk, *Modern Russian and Chinese Integrated Air Defence Systems: The Nature of the Threat, Growth Trajectory and Western Options*, RUSI Occasional Paper (London: Royal United Services Institute, January 2020), <https://www.rusi.org/explore-our-research/publications/occasional-papers/modern-russian-and-chinese-integrated-air-defence-systems-nature-threat-growth-trajectory-and>. For Tor-M2, see "9K330 Tor (SA-15 Gauntlet) Russian Short-Range Surface-to-Air Missile System," *Worldwide Equipment Guide*, U.S. Army OE Data Integration Network (ODIN), accessed September 2, 2026, [https://odin.t2com.army.mil/WEG/Asset/9K330_Tor_\(SA-15_Gauntlet\)_Russian_Short-Range_Surface-to-Air_Missile_System](https://odin.t2com.army.mil/WEG/Asset/9K330_Tor_(SA-15_Gauntlet)_Russian_Short-Range_Surface-to-Air_Missile_System); and "Latest Tor-M2 Anti-Aircraft Missile Systems Arrive for Russia's Baltic Fleet," TASS, October 31, 2019, <https://tass.com/defense/1086312>. On pre-2019 Tor-M1 in Kaliningrad, see Marek Żyła, "Kaliningrad Oblast in the Military System of the Russian Federation," *Security and Defence Quarterly* 25, no. 3 (June 2019): <https://doi.org/10.35467/sdq/105636>.
- 151 "Chapter III: Russian and NATO Surface Capabilities in the High North," *Whitehall Papers* 100, no. 1 (2022): 42-67, <https://doi.org/10.1080/02681307.2022.2030967>.
- 152 Praveen Duddu, "Project 22800 Karakurt-Class Corvettes," *Naval Technology*, September 11, 2017, <https://www.naval-technology.com/projects/project-22800-karakurt-class-corvettes/>.
- 153 Robin Ashby and Joseph E. Fallon, "The Baltic Fleet: Encircled and Constrained," *Defence Viewpoints*, March 23, 2024, updated April 2026, <https://www.defenceviewpoints.co.uk/articles-and-analysis/the-baltic-fleet-encircled-and-constrained>; bmpd, "В Калининграде сформировано управление 132-й смешанной

- авиационной дивизии” [In Kaliningrad, the command of the 132nd Composite Aviation Division has been formed], bmpd (blog), May 11, 2019, <https://bmpd.livejournal.com/3639474.html>; and Scramble, “Russian Federation Naval Aviation,” Scramble, accessed June 10, 2026, <https://scramble.nl/planning/orbats/russian-federation/russian-federation-naval-aviation#MWB244>; and “Russian Navy’s New Su-30SM2 Fighters Lead Baltic Fleet Exercises Simulating Strikes on NATO Targets,” *Military Watch Magazine*, June 9, 2026, <https://militarywatchmagazine.com/article/russian-navy-su30sm2-baltic-exercises>.
- 154 Justin Bronk, *Russian Combat Air Strengths and Limitations: Lessons from Ukraine* (Alexandria, VA: CNA, April 2023), <https://www.cna.org/reports/2023/04/Russian-Combat-Air-Strengths-and-Limitations.pdf>; Justin Bronk, *The Evolution of Russian and Chinese Air Power Threats*, RUSI Insights Paper (London: Royal United Services Institute, January 2026), <https://www.rusi.org/explore-our-research/publications/insights-papers/evolution-russian-and-chinese-air-power-threats>; Iwona Wiśniewska et al., *Kaliningrad Oblast 2016: The Society, Economy and Army*, OSW Report 12/2016 (Warsaw: Centre for Eastern Studies, December 2016), https://www.osw.waw.pl/sites/default/files/raport_in_the_kaliningrad_net.pdf; Ivan Khomenko, “French Rafales Scramble to Intercept Russian Su-30 Fighters Near NATO Airspace,” UNITED24 Media, May 30, 2026, <https://united24media.com/war-in-ukraine/french-rafales-scramble-to-intercept-russian-su-30-fighters-near-nato-airspace-19336>; David Axe, “Russia’s Su-27 Fighters Wreak Absolute Havoc in the Baltics,” *National Interest*, September 16, 2021, <https://nationalinterest.org/blog/reboot/russias-su-27-fighters-wreak-absolute-havoc-baltics-193901>; and U.S. Army TRADOC G-2, “R-37M,” Worldwide Equipment Guide, Operational Environment Data Integration Network (ODIN), accessed September 1, 2026, <https://odin.t2com.army.mil/WEG/Asset/59940359ebacd5953098f01ece89c21e>.
- 155 OE Data Integration Network (ODIN), “Murmansk-BN Russian Long-Range Communications Jamming System,” ODIN, modified June 5, 2025, <https://odin.t2com.army.mil/WEG/Asset/b4cd1efd5c57c88bcfe-7ca78a2831903>; Timothy Thomas, *Russia’s Electronic Warfare Force: Blending Concepts with Capabilities*, Report 19-2714 (McLean, VA: MITRE Center for Technology and National Security, September 2020), <https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf>; Vadim Kushnikov, “Russia Is Testing Electronic Warfare System in Kaliningrad,” *Militarnyi*, January 18, 2024, <https://militarnyi.com/en/news/russia-is-testing-electronic-warfare-system-in-kaliningrad/>; and “What Is Russian EW System in Kaliningrad That’s Haunting Poland and Baltics,” *Defense Express*, July 7, 2025, https://en.defence-ua.com/news/what_is_the_russian_ew_system_in_kaliningrad_thats_haunting_poland_and_the_baltics-15062.html.
- 156 Tiash Saha, “Krasukha Electronic Warfare (EW) System, Russia,” *Army Technology*, January 5, 2024, <https://www.army-technology.com/projects/krasukha-electronic-warfare-ew-system-russia/>.
- 157 Konrad Muzyka, *Russian Forces in the Western Military District*, Occasional Paper (Alexandria, VA: CNA, December 2020), <https://www.cna.org/reports/2021/06/Russian-Forces-in-the-Western-Military-District.pdf>; Athanasios Sdrakas, “An MDO Approach to NATO’s Counter-IADS Strategy: Integrating Suppression of Enemy Air Defences and Cyber-Electromagnetic Activities,” *JAPCC Journal* 41 (April 2026), <https://www.japcc.org/articles/an-mdo-approach-to-natos-counter-iads-strategy/>.
- 158 *Army Technology*, “S-400 Triumph”; “92N6E ‘Grave Stone’,” *Radartutorial.eu*, accessed June 10, 2026, <https://www.radartutorial.eu/19.kartei/06.missile/karte006.en.html>.
- 159 Wayne P. Hughes and Robert P. Girrier, *Fleet Tactics and Naval Operations*, Third Edition (Annapolis, MD: Naval Institute Press, 2018); Joint Staff, *Command and Control for Joint Maritime Operations*, Joint Publication 3-32 (Arlington, VA: Joint Chiefs of Staff, August 2013), https://edocs.nps.edu/2012/December/jp3_32.pdf; and Department of the Navy, *Naval Warfare, Naval Doctrine Publication 1* (Arlington, VA: Navy, Marine Corps, Coast Guard, April 2020), https://cimsec.org/wp-content/uploads/2020/08/NDP1_April2020.pdf.
- 160 Joint Staff, *Command and Control for Joint Maritime Operations*; NATO, *Allied Joint Doctrine for Maritime Operations*, Allied Joint Publication-3.1, Edition B, Version 1 AJP-3.1 (Brussels: NATO Standardization Office (NSO), April 2025), <https://assets.publishing.service.gov.uk/media/67f3b07d53505b2ca44efeed/>

AJP_3.1_Maritime_Ops_EdB.pdf; and Michael Manning, “Sea Control: Feasible, Acceptable, Suitable, or Simply Imperative,” *Journal of Advanced Military Studies* 11, no. 2 (2020): 51–73, https://www.usmcu.edu/Portals/218/3_Manning_JAMS.pdf.

- 161 Department of the Navy, *Naval Warfare*, Naval Doctrine Publication 1.
- 162 John Worry, *Warfare in the Classical World* (London: Salamander Books, 1980).
- 163 Alfred Mahan, *The Influence of Sea Power upon History, 1660–1783* (Boston: Little, Brown, 1890); and Julian S. Corbett, *Some Principles of Maritime Strategy* (London: Longmans, Green, 1911).
- 164 Arne Røksund, *The Jeune École: The Strategy of the Weak* (Leiden: Brill, 2007); and John Dotson, “The Jeune Ecole Offers Lessons for a New Contested Maritime Environment,” *Naval History* 38, no. 4 (August 2024), <https://www.usni.org/magazines/naval-history/2024/august/jeune-ecole-offers-lessons-new-contested-maritime-environment>.
- 165 Hughes and Girrier, *Fleet Tactics and Naval Operations*; Chief of Naval Operations, *Navigation Plan 2024: For America’s Warfighting Navy 2024* (Arlington, VA: Department of the Navy, 2024), 14–15, <https://www.navy.mil/Portals/1/CNO/NAVPLAN2024/Files/CNO-NAVPLAN-2024-high-res-v2.pdf>; Ronald O’Rourke, “Defense Primer: Navy Distributed Maritime Operations (DMO) Concept,” Congressional Research Service, IF12599, December 4, 2025, <https://www.congress.gov/crs-product/IF12599>; U. S. Naval Institute Staff, “Defense Primer: Navy Distributed Maritime Operations Concept,” *USNI News*, September 12, 2025, <https://news.usni.org/2025/09/12/defense-primer-navy-distributed-maritime-operations-concept>; and Dmitry Filipoff, *Distributed Maritime Operations: Solving What Problems and Seizing Which Opportunities?* (Washington, DC: Atlantic Council, July 2024), <https://www.atlanticcouncil.org/wp-content/uploads/2024/06/Distributed-Maritime-Operations-Solving-what-problems-and-seizing-which-opportunities.pdf>.
- 166 Department of Defense, *Military and Security Developments Involving the People’s Republic of China*, Annual Report to Congress (Arlington, VA: Department of Defense, 2023), <https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF>; David C. Logan, *China’s Sea-Based Nuclear Deterrent: Organizational, Operational, and Strategic Implications*, CMSI China Maritime Report no. 33 (Newport, RI: CMSI, November 30, 2023), <https://digital-commons.usnwc.edu/cmsi-maritime-reports/33>; and Matthew P. Funaiolo, Joseph S. Bermudez Jr., and Brian Hart, “A Glimpse of Chinese Ballistic Missile Submarines,” *CSIS, Commentary*, August 4, 2021, <https://www.csis.org/analysis/glimpse-chinese-ballistic-missile-submarines>.
- 167 Ross Babbage, *Countering China’s Adventurism in the South China Sea* (Washington, DC: CSBA, December 2016), <https://csbaonline.org/research/publications/countering-chinas-adventurism-in-the-south-china-sea-strategy-options-for-t>.
- 168 Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People’s Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR1708.html.
- 169 Dolma Tsering, “China’s ‘Undersea Great Wall’ Project: Implications,” *National Maritime Foundation*, December 9, 2016, <https://maritimeindia.org/chinas-undersea-great-wall-project-implications/>; and Gabriel Honrada, “China’s Undersea Great Wall Targets US Sub Supremacy,” *Asia Times*, March 3, 2026, <https://asiatimes.com/2026/03/chinas-undersea-great-wall-targets-us-sub-supremacy/>.
- 170 Benjamin Jensen, Mackenzie Eaglen, Henry H. Carroll, and Harold “Bud” Bishop, *Flipping the Script: How to Hold China’s New Carriers at Risk* (Washington, DC: CSIS, August 2026), <https://www.csis.org/analysis/flipping-script-how-hold-chinas-new-carriers-risk>.
- 171 “China Island Tracker,” *Asia Maritime Transparency Initiative*, CSIS, accessed May 7, 2026, <https://amti.csis.org/island-tracker/china/>.

- 172 Arne Røksund, *The Jeune École: The Strategy of the Weak*, History of Warfare 44 (Leiden: Brill, 2007).
- 173 On the concept of emergence in complex systems, see Ben Zweibelson, “Understanding Emergence: How Complexity Theory Requires Getting Out of the Military’s Favored Newtonian Box,” Medium, April 15, 2022, <https://benzweibelson.medium.com/understanding-emergence-how-complexity-theory-requires-getting-out-of-the-militarys-favored-bf914e06f1e>.
- 174 Geoffrey Till, “The Nelson Touch: An Effects Based Approach?,” *Naval Review* 93, no. 4 (2005): 320, reprinted October 21, 2023, <https://www.naval-review.com/news-views/the-nelson-touch-an-effects-based-approach/>.
- 175 Rudraksh Pathak, “Asymmetry Rising: How Autonomous Systems Enforce Sea Denial,” Center for International Maritime Security (CIMSEC), March 30, 2026, <https://cimsec.org/asymmetry-rising-how-autonomous-systems-enforce-sea-denial-on-high-value-targets/>.
- 176 Office of the Chief of Naval Operations, *U.S. Navy Fighting Instructions* (Washington, DC: Office of the Chief of Naval Operations, February 2026), <https://media.defense.gov/2026/Feb/06/2003871752/-1/-1/1/CNO%20FIGHTING%20INSTRUCTIONS.PDF>.
- 177 China Maritime Studies Institute (CMSI), “CMSI China Maritime Reports,” U.S. Naval War College Digital Commons, accessed May 27, 2026, <https://digital-commons.usnwc.edu/cmsi-maritime-reports/>.
- 178 Thomas G. Mahnken et al., *Tightening the Chain: Implementing a Strategy of Maritime Pressure in the Western Pacific* (Washington, DC: CSBA, 2019), https://csbaonline.org/uploads/documents/Tightening_the_Chain_web_Final.pdf.
- 179 Hughes and Girrier, *Fleet Tactics and Naval Operations*.
- 180 Engstrom, *Systems Confrontation and System Destruction Warfare*.
- 181 Jan van Tol, Mark Gunzinger, Andrew F. Krepinevich, and Jim Thomas, *AirSea Battle: A Point-of-Departure Operational Concept* (Washington, DC: CSBA, 2010), <https://csbaonline.org/resource/airsea-battle-a-point-of-departure-operational-concept/>.
- 182 James M. Acton ed., *Entanglement: Chinese and Russian Perspectives on Non-Nuclear Weapons and Nuclear Risks* (Washington, DC: Carnegie Endowment for International Peace, November 2017), https://assets.carnegieendowment.org/static/files/Entanglement_interior_FNL.pdf.
- 183 Carl von Clausewitz, *On War*, Book 6, Chapter 1, “Offence and Defence,” trans. J. J. Graham (London: N. Trübner, 1873), <https://clausewitzstudies.org/readings/OnWar1873/BK6ch01.html>; and Sumida, “On Defense as the Strongest Form of War.”
- 184 Department of the Army, *Tactics, Field Manual (FM) 3-90* (Arlington, VA: Department of the Army, May 2023), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN38160-FM_3-90-000-WEB-1.pdf.
- 185 Dwight D. Oland, *North Apennines: The U.S. Army Campaigns of World War II*, Brochure CMH Pub 72-34 (Fort McNair: U.S. Army Center of Military History, [1996]), <https://history.army.mil/portals/143/Images/Publications/catalog/72-34.pdf>.
- 186 Jack Watling and Nick Reynolds, *Tactical Developments During the Third Year of the Russo-Ukrainian War* (London: Royal United Services Institute, 2025), <https://static.rusi.org/tactical-developments-third-year-russo-ukrainian-war-february-2205.pdf>.
- 187 Jack Watling and Nick Reynolds, *Stormbreak: Fighting Through Russian Defences in Ukraine’s 2023 Offensive* (London: Royal United Services Institute, September 4, 2023), <https://www.rusi.org/explore-our-research/publications/special-resources/stormbreak-fighting-through-russian-defences-ukraines-2023-offensive>.

- 188 Eric Rosenbach et al., “Russian Threats to NATO’s Eastern Flank: Scenarios, Strategy, and Policy for European Security,” Belfer Center for Science and International Affairs, February 5, 2026, <https://www.belfercenter.org/research-analysis/russia-nato-baltics-scenarios-europe-security>; and Jennifer Kavanagh and Jeremy Shapiro, “The Bear in the Baltics: Reassessing the Russian Threat in Estonia,” European Council on Foreign Relations, December 18, 2025, <https://ecfr.eu/publication/the-bear-in-the-baltics-reassessing-the-russian-threat-in-estonia/>.
- 189 Rosenbach et al., “Russian Threats to NATO’s Eastern Flank.”
- 190 John Letzing, “Suwalki Gap: The Tiny Bit of Europe with Big Implications,” World Economic Forum, July 12, 2022, <https://www.weforum.org/stories/2022/07/suwalki-gap-russia-belarus-lithuania-sanctions-ukraine/>.
- 191 David A. Shlapak and Michael Johnson, *Reinforcing Deterrence on NATO’s Eastern Flank: Wargaming the Defense of the Baltics* (Santa Monica, CA: RAND Corporation, January 2016), https://www.rand.org/pubs/research_reports/RR1253.html.
- 192 Scott Boston et al., *Assessing the Conventional Force Imbalance in Europe: Implications for Countering Russian Local Superiority* (Santa Monica, CA: RAND Corporation, February 2018), https://www.rand.org/pubs/research_reports/RR2402.html.
- 193 Ben Hodges, Janusz Bugajski, and Peter B. Doran, *Securing the Suwalki Corridor: Strategy, Statecraft, Deterrence, and Defense* (Washington, DC: Center for European Policy Analysis, July 2018), <https://www.scribd.com/document/447193822/CEPA-Securing-the-Suwalki-Corridor-pdf>
- 194 Eric Rosenbach et al., *Russian Threats to NATO’s Eastern Flank: Scenarios, Strategy, and Policy for European Security* (Cambridge, MA: Belfer Center, February 2026), [https://www.belfercenter.org/sites/default/files/2026-02/Belfer_Russian Threats_3.1.pdf](https://www.belfercenter.org/sites/default/files/2026-02/Belfer_Russian%20Threats_3.1.pdf).
- 195 Dmitry (Dima) Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War* (Stanford, CA: Stanford University Press, 2024).
- 196 “Russian Firepower Strike Tracker: Analyzing Missile Attacks in Ukraine,” CSIS Futures Lab, accessed May 9, 2026, <https://www.csis.org/programs/futures-lab/projects/russian-firepower-strike-tracker-analyzing-missile-attacks-ukraine>.
- 197 “Ukraine’s Intelligence Reports Major Upgrades to Russian Lancet Drone,” New Voice of Ukraine (NV), March 23, 2026, <https://english.nv.ua/nation/lancet-drone-with-artificial-intelligence-updates-western-details-and-risks-50594148.html>; Iryna Lutsak, “Cheap and Dangerous: How the Molniya Plywood Drone Turned into a Big Problem for the Defense Forces,” Mezha (Defense), January 6, 2026, <https://oboronka.mezha.ua/en/udarni-droni-molniya-harateristiki-chim-nebezpechni-307515/>; and Kollen Post, “Putin’s Glide Bombs Are Turning Ukraine’s Fortress City into Rubble,” *Boston Herald*, June 27, 2026, <https://www.bostonherald.com/2026/06/27/putins-glide-bombs-are-turning-ukraines-fortress-city-into-rubble/>.
- 198 Watling and Reynolds, *Stormbreak*; Seth G. Jones, Alexander Palmer, and Joseph S. Bermudez Jr., “Ukraine’s Offensive Operations: Shifting the Offense-Defense Balance,” CSIS, *CSIS Briefs*, June 9, 2023, <https://www.csis.org/analysis/ukraines-offensive-operations-shifting-offense-defense-balance>.
- 199 Richard L. Garcia and Colin Colley, “Russian Minefield Tactics Pose Challenge to Mobility,” T2COM G2 Operational Environment Enterprise, November 13, 2024, <https://oe.t2com.army.mil/product/russian-minefield-tactics-pose-challenge-to-mobility/>; and Charles Bartles, “Russia Fields the ‘Zemledeliye’ Engineering System for Remote Mining,” OE Watch, Foreign Military Studies Office, April 2022, <https://oe.t2com.army.mil/product/russia-fields-the-zemledeliye-engineering-system-for-remote-mining/>.

- 200 David Axe, "The Russians Installed a GPS Jammer in Ukraine. The Ukrainians Blew It Up with a GPS-Guided Bomb," *Forbes*, October 31, 2023, <https://www.forbes.com/sites/davidaxe/2023/10/31/the-russians-installed-a-gps-jammer-in-ukraine-the-ukrainians-blew-it-up-with-a-gps-guided-bomb/>; and "R-330Zh Zhitel Russian Cellular Jamming and Direction Finding System," Operational Environment Data Integration Network, U.S. Army Training and Doctrine Command, accessed July 7, 2026, https://odin.tradoc.army.mil/mediawiki/index.php/R-330Zh_Zhitel_Russian_Cellular_Jamming_and_Direction_Finding_System.
- 201 Luke P. High, "Sustaining Reconnaissance," *Army.mil*, January 7, 2015, https://www.army.mil/article/140110/sustaining_reconnaissance.
- 202 Brandi Vincent, "Southcom Creates New Autonomous Warfare Command to Build Up Its Drone Prowess," *DefenseScoop*, April 22, 2026, <https://defensescoop.com/2026/04/22/southcom-new-autonomous-warfare-command-drones-gen-donovan/>.
- 203 Ministry of Defence of Ukraine, "The 'Drone Line' Project Has Been Launched in the Defence Forces of Ukraine to Develop UAV-Operating Units," news release, March 3, 2025, <https://mod.gov.ua/en/news/the-drone-line-project-has-been-launched-in-the-defence-forces-of-ukraine-to-develop-uav-operating-units>; Ministry of Defence of Ukraine, "Drone Line: Implementing a New Warfare Doctrine," news release, April 9, 2026, <https://mod.gov.ua/en/news/drone-line-implementing-a-new-warfare-doctrine>; "Ukraine Says It Is Employing New Integrated Drone-Infantry Warfare System," *Reuters*, April 15, 2026, <https://www.reuters.com/business/aerospace-defense/ukraine-says-it-is-employing-new-integrated-drone-infantry-warfare-system-2026-04-15/>; "Russia's Putin Calls for Quick Development of Drone Forces," *Reuters*; Osborn, "Russia Woos Students for Its Drone Forces in Ukraine with Large Financial Packages"; DuPont et al., "Red Skies Ahead"; and "Ukraine's Top Commander Says Russia Plans Big Boost in Drone Production," *Reuters*.
- 204 Kateryna Bondar, "Why Ukraine Is Establishing Unmanned Forces Across Its Defense Sector and What the United States Can Learn from It," *CSIS, Commentary*, November 19, 2024, <https://www.csis.org/analysis/why-ukraine-establishing-unmanned-forces>; President of Ukraine, "I Signed a Decree Initiating the Establishment of a Separate Branch of Forces—The Unmanned Systems Forces—Address by the President of Ukraine," Official Website of the President of Ukraine, transcript, February 6, 2024, <https://www.president.gov.ua/en/news/pidpisav-ukaz-yakij-rozpochinaye-stvorennya-okremogo-rodu-si-88817>; and Ministry of Defence of Ukraine, "The USF Command Has Been Granted the Authority to Act as a Procurement Body for UAVs and EW Systems, Following the MoD and SSCS Procurements," press release, October 29, 2024, <https://mod.gov.ua/en/news/the-command-of-the-unmanned-systems-forces-has-been-granted-the-authority-to-act-as-a-procurement-body-for-ua-vs-and-electronic-warfare-systems-following-the-ministry-of-defense-and-state-special-communications-service-procureme>.
- 205 "Drone Line: Implementing a New Warfare Doctrine," Ministry of Defence of Ukraine, April 9, 2026, <https://mod.gov.ua/en/news/drone-line-implementing-a-new-warfare-doctrine>; and "The \$880M Drone Line: How Ukraine Built the Ultimate Tech Shield," *Digital State UA*, March 5, 2026, <https://digitalstate.gov.ua/news/tech/liniia-droniv-iak-880-mln-peretvoryly-bezpilotnyky-na-osnovu-suchasnoyi-viyny>.
- 206 "Russia's Putin Calls for Quick Development of Drone Forces," *Reuters*, updated June 12, 2025, <https://www.reuters.com/business/aerospace-defense/russias-putin-calls-quick-development-drone-forces-2025-06-12/>; Andrew Osborn, "Russia Woos Students for Its Drone Forces in Ukraine with Large Financial Packages," *Reuters*, updated April 2, 2026, <https://www.reuters.com/world/europe/russia-woos-students-its-drone-forces-ukraine-with-large-financial-packages-2026-04-02/>; Ian DuPont et al., "Red Skies Ahead: Russia Planning for Its Drone-Driven Army of Tomorrow," *Military Review* (January-February 2026): 1-10, <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/January-February-2026/Red-Skies-Ahead/>; and "Ukraine's Top Commander Says Russia Plans Big Boost

- in Drone Production,” Reuters, updated January 18, 2026, <https://www.reuters.com/world/ukraines-top-commander-says-russia-plans-big-boost-drone-production-2026-01-18/>.
- 207 Ministry of Defence of Ukraine, “Drones, Cybersecurity, Rehabilitation: Higher Military Educational Institutions Are Intensifying Training in Modern Disciplines While Introducing New Fields of Study,” news release, February 4, 2025, <https://mod.gov.ua/en/news/drones-cybersecurity-rehabilitation-higher-military-educational-institutions-are-intensifying-training-in-modern-disciplines-while-introducing-new-fields-of-study>; and Ministry of Defence of Ukraine, “Scaling Up the Aviation Personnel Training System in 2025,” news release, January 2, 2026, <https://mod.gov.ua/en/news/scaling-up-the-aviation-personnel-training-system-in-2025>.
- 208 “Russia’s Putin Calls for Quick Development of Drone Forces,” Reuters; Osborn, “Russia Woos Students for Its Drone Forces in Ukraine with Large Financial Packages”; DuPont et al., “Red Skies Ahead”; and “Ukraine’s Top Commander Says Russia Plans Big Boost in Drone Production,” Reuters.
- 209 Office of the Under Secretary of Defense for Policy, “DoD Directive 5132.03: DoD Policy and Responsibilities Relating to Security Cooperation,” Department of Defense, December 29, 2016, https://open.defense.gov/portals/23/Documents/foreignasst/DoDD_513203_on_Security_Cooperation.pdf.
- 210 Office of the DoD Chief Information Officer, “DoD Instruction 8110.01: Mission Partner Environment Information Sharing Capability Implementation for the DoD,” Department of Defense, June 30, 2021, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/811001p.pdf>.
- 211 Michael Marrow, “Pay the PIPIR: DoD Launching New Indo-Pacific Partnership for Buying, Sustaining Weapons,” Breaking Defense, August 8, 2024, <https://breakingdefense.com/2024/08/pay-the-pipir-dod-launching-new-indo-pacific-partnership-for-buying-sustaining-weapons/>; and Luke A. Nicastro, *AUKUS Pillar 2 (Advanced Capabilities): Background and Issues for Congress*, CRS Report R47599 (Washington, DC: Congressional Research Service, May 21, 2024), <https://www.congress.gov/crs-product/R47599>.
- 212 “DOD Lays Out Plan to Implement National Defense Industrial Strategy,” Department of Defense, October 29, 2024, <https://www.war.gov/News/News-Stories/Article/Article/3949630/dod-lays-out-plan-to-implement-national-defense-industrial-strategy/>; and Department of Defense, “DOD Releases First-Ever National Defense Industrial Strategy,” press release, January 11, 2024, <https://www.war.gov/News/Releases/Release/Article/3643326/dod-releases-first-ever-national-defense-industrial-strategy/>.
- 213 10 U.S.C. § 3771.
- 214 Chairman of the Joint Chiefs of Staff, Joint Publication 4-0, Joint Logistics, change 1, May 22, 2025, <https://www.jcs.mil/Doctrine/Joint-Doctrine-Pubs/4-0-Logistics-Series/>.
- 215 Department of Defense, “DOD Releases First-Ever National Defense Industrial Strategy”; and Department of Defense, “DOD Lays Out Plan to Implement National Defense Industrial Strategy.”
- 216 10 U.S.C. § 4401, “Requirement for Modular Open System Approach in Major Defense Acquisition Programs; Definitions,” text contains laws in effect on May 10, 2026, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section4401&num=0&edition=prelim>.
- 217 10 U.S.C. § 4403, “Requirements Relating to Availability of Major System Interfaces and Support for Modular Open System Approach,” text contains laws in effect on May 10, 2026, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section4403&num=0&edition=prelim>.
- 218 10 U.S.C. § 3771, “Rights in Technical Data: Regulations,” text contains laws in effect on May 10, 2026, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section3771&num=0&edition=prelim>.

- 219 Department of Defense, “DOD Announces Publication of the Intellectual Property Guidebook for DOD Acquisition,” press release, May 1, 2025, <https://www.war.gov/News/Releases/Release/Article/4172048/dod-announces-publication-of-the-intellectual-property-guidebook-for-dod-acquis/>; and Office of the Under Secretary of Defense for Acquisition and Sustainment, *Intellectual Property Guidebook for DoD Acquisition* (Washington, DC: Department of Defense, April 2025), https://arpa-h.gov/sites/default/files/2025-05/DoD%20_IP_Guidebook_Apr2025.pdf.
- 220 Department of Defense, *Software Modernization Implementation Plan FY 25-26* (Arlington, VA: Department of Defense, May 2025), <https://dodcio.defense.gov/Portals/0/Documents/Library/SW-Mod-I-Plan25-26.pdf>; and Office of Prepublication and Security Review, DoD Enterprise DevSecOps Fundamentals, Version 2.5 (Arlington, VA: Department of Defense, October 2024), <https://dodcio.defense.gov/Portals/0/Documents/Library/DoD%20Enterprise%20DevSecOps%20Fundamentals%20v2.5.pdf>.
- 221 Department of Defense, *Fiscal Year (FY) 2026 Budget Estimates: Army: Justification Book Volume 4d of 4: Research, Development, Test & Evaluation, Army: Budget Activity 9*.
- 222 Department of the Army, “U.S. Army Taps Three Companies for Cutting-Edge Launched Effects Demonstration”; and Cheryl Marino, “Launched Effects Program Accelerates Battlefield Reach,” U.S. Army, May 22, 2026, https://www.army.mil/article/291696/launched_effects_program_accelerates_battlefield_reach.
- 223 Department of Defense, *Fiscal Year (FY) 2026 Budget Estimates: Army: Justification Book Volume 4d of 4: Research, Development, Test & Evaluation, Army: Budget Activity 9* (Arlington, VA: Department of Defense, June 2025), <https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2026/Discretionary%20Budget/rdte/RDTE%20-%20Vol%204%20-%20Budget%20Activity%209.pdf>.
- 224 Clark, “Defense Innovation Official”; and Department of Defense, “Deputy Secretary of Defense Kathleen Hicks Announces Additional Replicator All-Domain Attributable Autonomous Capabilities,” press release, November 13, 2024, <https://www.war.gov/News/Releases/Release/Article/3963289/deputy-secretary-of-defense-kathleen-hicks-announces-additional-replicator-all/>.
- 225 10 U.S.C. § 4022, “Authority of the Department of Defense to Carry Out Certain Prototype Projects,” laws in effect on May 10, 2026, [https://uscode.house.gov/view.xhtml?req=\(title:10 section:4022 edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:10 section:4022 edition:prelim)); 10 U.S.C. § 4401, “Requirement for Modular Open System Approach in Major Defense Acquisition Programs; Definitions,” laws in effect on May 10, 2026, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section4401&num=0&edition=prelim>; Federal Acquisition Regulation, Title 48, Chapter 1, Subchapter C, Part 16, Subpart 16.5, “Subpart 16.5—Indefinite-Delivery Contracts,” Code of Federal Regulation (eCFR), April 25, 2000, <https://www.ecfr.gov/current/title-48/chapter-1/subchapter-C/part-16/subpart-16.5>.
- 226 10 U.S.C. § 4022; Defense Federal Acquisition Regulation Supplement (DFARS), “206.001-70: Exception for Prototype Projects for Follow-on Production Contracts,” DFARS Change 11/10/2025, effective November 10, 2025, <https://www.acquisition.gov/dfars/206.001-70-exception-prototype-projects-follow-production-contracts>.
- 227 Marino, “Launched Effects Program Accelerates Battlefield Reach.”
- 228 10 U.S.C. § 3602; and Office of the Under Secretary of Defense for Acquisition and Sustainment, *Operation of the Middle Tier of Acquisition*.
- 229 Richard Newton, “Bridging the Valley of Death and Thriving Beyond—Improving Transition Success with Metrics,” *Defense Acquisition Magazine*, July–August 2022, <https://www.dau.edu/library/damag/july-august2022/bridging-valley-death>.
- 230 10 U.S.C. § 3501, “Multiyear Contracts: Acquisition of Property,” text contains laws in effect on May 10, 2026, <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title10-section3501&num=0&edition=prelim>.

- 231 United States Space Force, *Space Warfighting: A Framework for Planners* (Washington, DC: Headquarters United States Space Force, April 2025), [https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/Space_Warfighting_-_A_Framework_for_Planners_BLK2_\(final_20250410\).pdf](https://www.spaceforce.mil/Portals/2/Documents/SAF_2025/Space_Warfighting_-_A_Framework_for_Planners_BLK2_(final_20250410).pdf); Erin Leon, “Space Is a Contested Domain,” U.S. Space Forces-Space, September 18, 2024, <https://www.spaceforces-space.mil/Newsroom/Article/3910216/space-is-a-contested-domain/>; Clayton Swope, Kari A. Bingen, Makena Young, and Kendra LaFave, *Space Threat Assessment 2025* (Washington, DC: CSIS, April 2025), <https://www.csis.org/analysis/space-threat-assessment-2025>.
- 232 Space Training and Readiness Command (STARCOM), *Space Force Doctrine Document 1, SFDD-1, The Space Force* (Arlington, VA: Space Force, April 2025), https://www.starcom.spaceforce.mil/Portals/2/Space%20Force%20Doctrine%20Document%201%20FINAL_4Apr25.pdf; and Department of Defense: *Military and Security Developments Involving the People’s Republic of China, Annual Report to Congress 2025* (Arlington, VA: Department of Defense, 2025), <https://media.defense.gov/2025/Dec/23/2003849070/-1/-1/1/ANNUAL-REPORT-TO-CONGRESS-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2025.PDF>.
- 233 David Daniels, “Apache Helicopter Integrates Launched Effects in Rapid Six-Month Development Effort,” U.S. Army, March 26, 2026, https://www.army.mil/article/291369/apache_helicopter_integrates_launched_effects_in_rapid_six_month_development_effort; and Katie Davis Skelley and DEVCOM Aviation & Missile Center Public Affairs, “New Capability Gives Apache Ability to Control Complex Unmanned Systems,” U.S. Army, April 8, 2026, https://www.army.mil/article/291612/new_capability_gives_apache_ability_to_control_complex_unmanned_systems.
- 234 Eve Sampson, “US Marine Corps Tests Using Helicopter as Mobile Drone Command Center,” *Marine Corps Times*, May 22, 2026, <https://www.marinecorpstimes.com/news/your-marine-corps/2026/05/22/us-marine-corps-tests-using-helicopter-as-mobile-drone-command-center/>.
- 235 “USAF Retires BACN EQ-4B Global Hawks,” Key.Aero, <https://www.key.aero/article/usaf-retires-bacn-eq-4b-global-hawks>; Theresa Hitchens and Michael Marrow, “Air Force Seeks to Scrap Its E-11 BACN Fleet,” *Breaking Defense*, April 30, 2026, <https://breakingdefense.com/2026/04/air-force-seeks-to-scrap-its-e-11-bacn-fleet/>; and Frank Wolfe, “Air Force to Retire BACN in 2028, Use Hybrid SATCOM Terminal as Bridge,” *Defense Daily*, April 30, 2026, <https://www.defensedaily.com/air-force-to-retire-bacn-in-2028-use-hybrid-satcom-terminal-as-bridge/air-force/>.
- 236 GA-ASI, “Modernized Gray Eagle® ER and Gray Eagle® STOL: The Gold Standard in MALE Unmanned Aircraft,” *Breaking Defense*, October 13, 2025, <https://breakingdefense.com/2025/10/modernized-gray-eagle-er-and-gray-eagle-stol-the-gold-standard-in-male-unmanned-aircraft/>; and Courtesy, “Army Advances Group 4+ S/VTOL Challenge,” U.S. Army, March 12, 2026, https://www.army.mil/article/291045/army_advances_group_4_svtol_challenge.
- 237 David Roza, “Air Force Names OA-1K Skyraider II as New Aircraft Prepares to Come Online,” *Air & Space Forces Magazine*, February 27, 2025, <https://www.airandspaceforces.com/air-force-oa-1k-skyraider-ii/>.
- 238 Department of the Air Force, *Agile Combat Employment*, Air Force Doctrine Note (AFDN) 1-21 (Arlington, VA: Department of the Air Force, August 23, 2022), https://www.doctrine.af.mil/Portals/61/documents/AFDN_1-21/AFDN%201-21%20ACE.pdf.



1616 Rhode Island Avenue NW, Washington, DC 20036
202.887.0200 | www.csis.org

FOLLOW CSIS

