Vol. 66, July 2026

MITCHELL INSTITUTE Policy Paper

Key Points

Point defense is necessary but insufficient to defend from the small UAV threat. Defeating this threat requires the employment of all aspects of counterair doctrine—both defensive and offensive efforts.

The counter–small UAV (C-sUAV) mission requires a system-of-systems approach, specifically a multi-layered and modular system synthesizing multi-spectral detection with kinetic and non-kinetic defeat technologies. Airborne sensors and effectors are essential to provide flexibility, survivability, and defense-in-depth in high-threat environments. These systems must be backstopped by integrated passive defenses that include hardening, dispersal, camouflage, deception, netting, and decoys.

Airmen must adopt a mindset of generating combat airpower while under threat and an ability to survive and operate (ATSO). Airmen across the base require timely threat awareness, orchestrated through a redesigned base defense operations center (BDOC). They must constantly balance force protection with mission accomplishment in a dynamic threat environment.

Small UAV proliferation requires deliberate and dynamic warfighter management of the electromagnetic (EM) spectrum. Due to the nature of the sUAV threat, the air base commander must consciously manage EM spectrum use within the air base and its immediate surroundings.

The U.S. government must provide the U.S. Air Force (USAF) with additional monetary and personnel support to effectively counter the sUAV threat. sUAV are a new threat and require the acquisition of new defensive technologies, the fielding of robust passive defenses, and the development of new defensive postures.

As a first step, the U.S. Air Force must fully resource air base point-defense systems into reconceptualized USAF command and control (C2) structures, complete with new training for the Airmen responsible for performing this critical mission and those expected to perform their regular duties while under sUAV attack.

Defeating the Drones: The Airman's Imperative to Defend from Small Uninhabited Aerial Vehicles

By Brig Gen Houston Cantwell, USAF (Ret.)
Senior Resident Fellow for Airpower Studies at the Mitchell Institute for Aerospace Studies

Abstract

Small uninhabited aerial vehicles (sUAV) present a rapidly evolving and proliferating air threat to expeditionary air bases and fielded forces. Because of their rapid innovation cycles, massive numbers, low-altitude flight paths, and varied physical characteristics, sUAV can circumvent traditional air defense systems. Combat operations in Ukraine demonstrate how these vehicles threaten airfields and fielded forces through persistence and mass, while attacks on U.S. forces across the Middle East during Operation Epic Fury illustrate their lethality.

Addressing this challenge requires more than improved point defense. U.S. air bases are critical weapons systems; defending them is integral to airpower generation, not a separate force-protection task. It demands a system-of-systems approach that integrates layered, multi-spectral detection with kinetic and non-kinetic effectors, supported by resilient command and control (C2) and deliberate electromagnetic spectrum management. High volumes of sUAV threats demand both defensive and offensive counter–sUAV capabilities to disrupt inbound threats as well as adversary production, launch sites, and C2 networks. This approach is rooted in counterair doctrine, and point defenses are simply not up to the task. The U.S. Air Force (USAF) must lead this reconceptualization of counter–sUAV operations to ensure kill chains are executed at speed, Airmen are trained and equipped for this mission, and airpower generation continues despite enduring sUAV threats.

Ultimately, the U.S. Air Force must relearn its ability to survive and operate under the persistent threat of attack given the proliferation of sUAV capabilities—to balance force protection with aircraft generation. Congress must provide the U.S. Air Force with the monetary and personnel resources it desperately needs to successfully defeat sUAV threats and maintain the United States' position as the global leader in airpower. The U.S. Air Force must focus its efforts, adapt its doctrine and procedures, and develop, integrate, and deploy the technology to counter the proliferating air threat posed by sUAV. Air base defense is core to the service's ability to generate airpower and must be prioritized to maximize aircraft generation, even in the face of sUAV attack.

Foreword

The growth of small uninhabited aerial vehicles (sUAV) is not a passing battlefield anomaly. It is inducing a structural change in the character of air base defense and, by extension, in the way the United States Air Force must think about generating combat power. For decades, American Airmen have operated from expeditionary bases where friendly control of the air largely shielded flightlines, maintenance crews, fuel farms, munitions storage, C2 nodes, and parked aircraft from persistent air attack. That condition can no longer be assumed.

The experience of Ukraine and recent U.S. operations makes one point unmistakable: The air base itself has become a central target set. Low-cost UAV can impose high operational and strategic costs when they disrupt sortie generation, damage scarce aircraft, or force commanders to trade mission accomplishment for force protection. This is not simply a force-protection problem, and it cannot be solved by adding isolated point-defense systems around a perimeter. It is a counterair problem that demands a counterair answer.

The solution must begin with layered defense, but it cannot end there. The U.S. Air Force must integrate multi-spectral detection, rapid identification, kinetic and non-kinetic defeat mechanisms, resilient command and control, passive defense, dispersal, deception, and electromagnetic spectrum discipline into a coherent system. At the same time, U.S. joint forces must attack the systems that generate the threat: production facilities, supply chains, storage sites, launch points, operators, datalinks, navigation sources, and C2 networks. Offense and defense are not competing approaches; they are mutually reinforcing elements of the same campaign.

Most importantly, Airmen must once again internalize the imperative to survive and operate. Generating aircraft while under attack is a demanding operational skill. It requires training, realistic exercises, clear authorities, real-time threat awareness, and a C2 construct built for speed. The base defense operations center must evolve from a ground-security node into an integrated air base defense hub. Air base commanders must have the tools, people, and authorities to fight the base as a weapon system.

This paper correctly argues that the sUAV challenge is not merely technical; it is doctrinal, organizational, operational, and cultural. The U.S. Air Force must lead this reconceptualization because the consequence of failure is measured not only in damaged equipment or lost infrastructure, but in lost sorties, lost initiative, and lost combat effectiveness. The nation must resource this mission accordingly. Airpower depends on the ability to generate it, and in the age of proliferated sUAV, that ability can no longer be taken for granted.

Lt Gen David A. Deptula, USAF (Ret.)
Dean, The Mitchell Institute for Aerospace Studies

Introduction

Small uninhabited aerial vehicles (sUAV) are a rapidly evolving, proliferating, and lethal air threat to U.S. expeditionary air bases and fielded forces. Because of their rapid innovation cycles, massive numbers, low-altitude flight paths, small signatures, and varied physical characteristics, sUAV can evade or overwhelm traditional air defense systems optimized for large aircraft and missiles. Recent combat operations in Ukraine demonstrate how sUAV threaten airfields and ground forces through persistence, mass, low cost, and adaptability. Attacks on U.S. bases across the Middle East during Operation Epic Fury further illustrate that even layered defenses can be penetrated, with potentially devastating consequences for aircraft on the ground, personnel, and infrastructure, ultimately reducing a base's ability to launch aircraft.

The United States Air Force must reconceptualize air base defense for the sUAV threat. Historically, U.S. Army air defense forces have provided critical protection for forward-deployed air bases, but legacy U.S. Army constructs are ineffective against sUAV threats. Modern air base defense must be optimized for sUAV and paired with a thoughtful offensive campaign and deliberate electromagnetic spectrum management. Future U.S. Air Force point defense efforts must integrate with U.S. Army systems, while optimizing for sUAV through multi-spectral detectors, resilient C2, kinetic and non-kinetic effectors, and a slew of passive defensive measures. Given the robust sUAV threat, traditional point defense is, on its own, insufficient and must be buttressed with a deliberate offensive counterair effort—striking the threat before it can get airborne. Ultimately, the increased reliance on datalinks and radio frequencies (RF) for sUAV operations and counter–sUAV operations highlights the importance of electromagnetic spectrum management. The risk of inadvertent electronic fratricide is at an all-time high and must be mitigated.

Despite improvements in air base defense, the proliferated sUAV threat demands an even more fundamental focus on balancing mission execution with survivability. For decades, Airmen have operated at expeditionary air bases with minimal concern for air threats. Warning sirens preceded the rare viable threat, and personnel took cover. The sUAV threat changes this calculus. It requires Airmen to focus on their ability to survive and operate. The expeditionary environment must honor the persistent sUAV threat by balancing the risk of attack with aircraft generation. Gone are the days of working an air base flightline without personal protective gear or real-time air threat awareness. Flightline operations must tie directly to threat detection to allow Airmen the ability to implement defensive measures commensurate with the actual threat. Airmen must adjust their mindset to generate airpower under varying levels of air threat.

Accordingly, this paper offers five central recommendations. First, the Department of Defense and Congress must provide the U.S. Air Force with the monetary and personnel resources required to develop and field essential C-sUAV capabilities, procedures, and postures. This includes fully resourcing air base point-defense systems, integrating U.S. Army ballistic missile defense capabilities where appropriate, and fielding systems for early warning, tracking, identification, and defeat. Second, the U.S. Air Force must adopt a layered system-of-systems approach that combines ground and airborne sensors, radio frequency detection, radar, acoustic sensors, electro-optical/infrared systems, electronic warfare, directed energy, guns, missiles, and low-cost drone interceptors. These systems must be modular, interoperable, and adaptable to match the pace of sUAV innovation. Third, the U.S. Air Force must transform air base C2. The base defense operations center (BDOC) must evolve from a ground-security node into an air defense C2 hub capable of managing the complete kill chain. This will require new training, new authorities, and the integration of air battle managers, weapons directors, and personnel with airspace-control expertise. Fourth, Airmen must learn to generate aircraft while under sUAV attack and incorporate an ability to survive and operate (ATSO) mentality. The U.S. Air Force should develop and exercise drone protection postures (DPP) that communicate threat levels across an installation and help commanders balance force protection, aircraft generation, passive defense, dispersal, sheltering, and emergency launch decisions. Fifth, the joint force must apply the full logic of counterair doctrine to the sUAV problem. Defensive point protection must be paired with offensive counterair operations that target adversary production facilities, supply chains, storage areas, launch sites, operators, datalinks, navigation systems, and C2 networks. At the same time, commanders must deliberately manage the electromagnetic spectrum, because both sUAV operations and C-sUAV systems depend heavily on RF energy, GPS, datalinks, jamming, sensing, and communications. Without disciplined spectrum management, friendly systems risk interfering with one another and undermining the very defenses they are meant to enable.

Failure to prepare for the growing sUAV threat exposes expeditionary air bases to an unrelenting air threat and jeopardizes their primary mission: generating airpower. The U.S. Air Force must therefore prioritize a counter–sUAV campaign composed of both defensive and offensive counterair efforts. Airmen must learn to survive and operate while under persistent sUAV threat. The U.S. Air Force can continue to provide decisive airpower to the Joint Force Commander despite a growing and formidable air threat by adapting procedures, integrating new technologies, and training Airmen to defend the air base while generating sorties.

sUAV Pose an Urgent Threat to U.S. Forces at Expeditionary Air Bases & Across the Battlespace

Small UAV have rapidly become a credible airborne method of attack, proving their effectiveness in both small and large numbers. The number of sUAV in combat has exploded into the tens of thousands in the past few years. At the end of 2023, U.S. forces stationed around the Middle East faced the constant threat of one-way, preprogrammed sUAV. The Shahed-101 and Shahed-136 were the most common threats, often striking in groups of one or two, and with larger attacks of up to five drones.[1] Though these relatively small numbers of sUAV had already proved formidable, massed sUAV attacks in the combat airspace of Ukraine demonstrated that sUAV have become an overwhelming threat. Figure 1 depicts the exponentially increasing use of Shahed drones against Ukraine since 2024. On July 9, 2025, Ukraine weathered a staggering attack of 741 Russian sUAV across the country in a single day.[2] Ukrainian Commander in Chief General Oleksandr Syrskyi reported that Russia launched 6,900 drones against Ukraine in September 2025 alone.[3] Reporting also indicates Ukraine shot down an impressive 33,000 drones in early March 2026.[4]

Given its high expenditure of drones against Ukraine, Russia pushed to maximize sUAV production in late 2025. Intelligence reports now estimate its output capability to be up to 2,700 drones per month.[5] Ukraine has responded in kind by ramping up production of defensive interceptor drones. "It's not an easy process, but by the end of November we expect to reach 600 to 800 interceptor drones per day, if nothing is disrupted," stated Ukrainian President Zelensky in November 2025.[6] Both the Russians and Ukrainians continue to intensify their proliferation of sUAV by increasing the numbers and the types of sUAV being used across the battlespace.

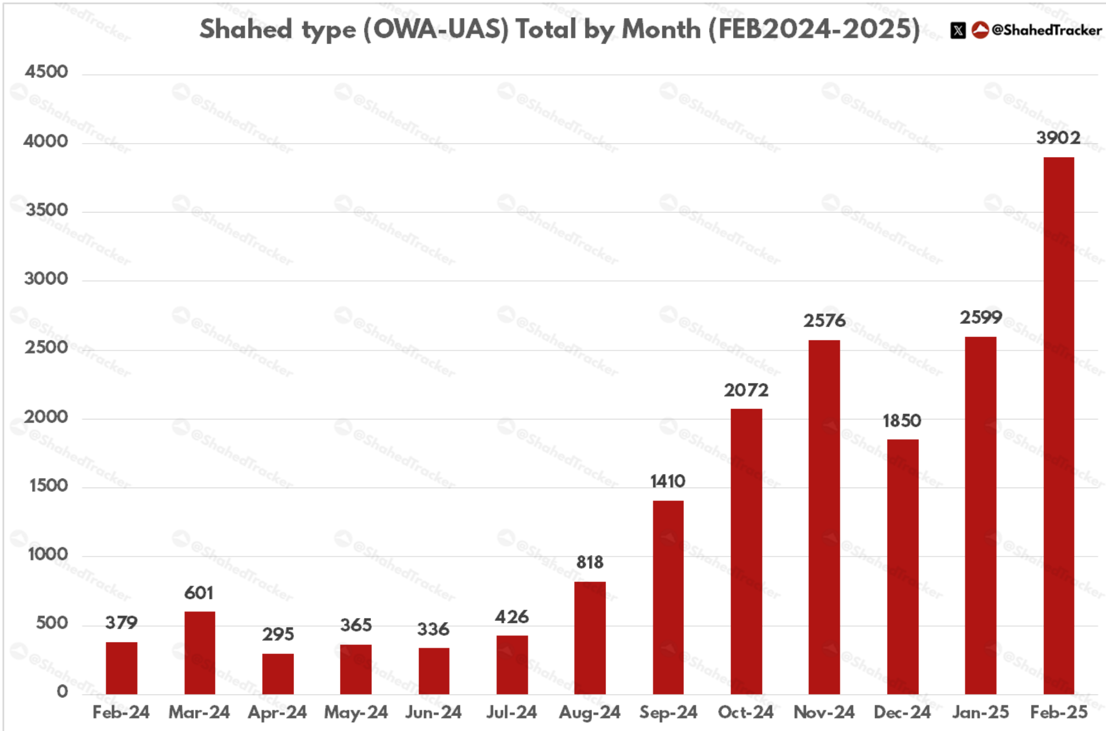

Figure 1: Number of Russian dones fired at Ukraine by month.

Chart from Shahed Tracker, "Shahed type OWA-UAS stats Feb2025," X, March 1, 2025.

On February 28, 2026, the U.S. military launched Operation Epic Fury "to dismantle the Iranian regime's security apparatus."[7] Drones have played significant roles for both sides, with the Department of Defense/War (DOD/W) publicly acknowledging U.S. employment of LUCAS one-way attack drones and Iran using nearly 1,000 drones altogether to attack U.S. and allied targets in the first six weeks of the conflict.[8] On March 27, 2026, in an attack that shocked the American public, Iran successfully destroyed a U.S. Air Force (USAF) E-3 Sentry AWACS C2 aircraft, injuring more than 10 service members and damaging several U.S. refueling aircraft in a combined missile and drone attack on Prince Sultan Air Base, Saudi Arabia.[9] Even six weeks after the start of Epic Fury, Tehran retained the ability to carry out 60–90 drone attacks a day, reflecting estimates of its pre-conflict drone supplies as being in the tens of thousands.[10]

Like Ukraine and Russia, Iran and the United States have pushed their own production capabilities of drones as offensive and defensive weapons. According to a Harvard Kennedy School analysis, Iran produces roughly 10,000 Shahed drones per month. Meanwhile, the U.S. government has contracted Lockheed Martin to increase annual PAC-3 interceptor production from around 600 to about 2,000, an undersized effort given the scale of the threat.[11] The United States must find a way of boosting capacity in a way that is both fiscally sustainable and scalable from a production perspective.

The relatively cheap cost and accessible technology of sUAV contribute heavily to the explosion of their use across the Ukrainian and Iranian battlespaces, illustrating the importance of considering cost-exchange ratios when calculating a response. Simple first-person view (FPV) drones cost as little as $400 and can precisely strike targets from miles away.[12] Shahed drones cost more but are still relatively inexpensive when compared to the technology typically used against them. Long-range Shaheds can fly over 1,000 miles and can carry a 100-pound

UA Category	Maximum Gross Takeoff Weight (lbs)	Normal Operating Altitude (ft)	Speed (KIAS)	Representative UAS
Group 1	0-20	< 1200 AGL	100 kts	WASP III, TACMAV RQ-14A/B, Buster, Nighthawk, RQ-11B, FPASS, RQ16A, Pointer, Aqua/Terra Puma
Group 2	21-55	< 3500 AGL	< 250	ScanEagle, Silver Fox, Aerosonde
Group 3	< 1320	< 18,000 MSL	< 250	RQ-7B Shadow, RQ-15 Neptune, XPV-1 Tern, XPV-2 Mako
Group 4	> 1320		Any Airspeed	MQ-5B Hunter, MQ-8B Fire Scout, MQ-1C Gray Eagle, MQ-1A/B/C Predator
Group 5	> 1320	> 18,000 MSL	Any Airspeed	MQ-9 Reaper, RQ-4 Global Hawk, RQ-4N Triton

Table 1: Joint UAV categorization chart.[53]

warhead, making them a credible threat to forces. And, while reports vary, a good rough estimate is that these Shaheds cost about $35,000 per drone.[13] Given the probability of hit and unit cost, Shaheds present the Russians with their most cost-effective option to strike static targets hundreds of miles into enemy territory.[14] Russia has also demonstrated that, by launching a large number of drones at single target areas, they can overwhelm defenses, allowing greater numbers to reach their targets.

Modern warfare has made it clear that sUAV (Groups 1 and 2) are credible threats to militaries equipped to defend against traditional fighter and bomber aircraft (See Table 1). Traditional aircraft are still important, as they offer distinct advantages—that is why the USAF, allied air forces, and the People's Liberation Army Air Force (PLAAF) are still building traditional combat aircraft. However, sUAV are adding a new dimension to air combat, which means the United States must expand the scale and scope of its airpower arsenal for both offensive and defensive purposes. The answer is "and," not "or."

The physical characteristics of sUAV—small size, airframe components, and power sources—when combined with their typical low-and-slow flight profiles, present distinct challenges to traditional counterair detect, track, identify, and engage capabilities.[15] Detecting their small physical size is a task in and of itself, but some airframes are composed of Styrofoam, further reducing their RF signature. Electric motors likewise reduce sUAV infrared (IR) signature. Even advanced missiles, such as the AIM-9L/M, are unable to track small aircraft propelled by electric motors due to a lack of IR signature.[16] Additionally, U.S. soldiers in the Middle East have had difficulty detecting

Category	System	Range	Speed	Typical Employment Altitude (ft)	Payload	Primary Use
Commercial off-the-shelf sUAV (COTS)	DJI Phantom / Mavic	5–15 km	50 km/hr	<300	<5 kg	ISR, small payload drop
Tactical ISR	Orlan-10	~120 km	130 km/hr	3–15K	Sensors	ISR, targeting
One-way Attack UAV	Shahed-Class	500–2,500+ km	250 km/hr	<1K	20–50kg warhead	One-way precision strike
MALE UAV	Bayraktar TB2	1,000+ km	300 km/hr	<24K	100–400kg Sensors / weapons	ISR and strike

Table 2: Threat sUAV.[54]

Continual Innovation

Continual innovation is an important theme of sUAV. Ukrainian military and industrial leaders have stated that new defensive technologies must be created every few weeks to keep pace with Russia's development of novel weapons.[55] Undoubtedly, Ukraine shows how modern warfare has become a contest to deploy attack drones adapted to fast-evolving enemy countermeasures. Warfighters engage directly with engineers, energizing an ongoing weapons evolution in a quest to remain one step ahead of their adversary. In many cases, teams of software engineers are embedded with the fielded forces, within one to two kilometers of the front lines, and often even living with the front-line soldiers.[56] As the Chief of the Swedish Air Force stated in late 2025, "Tactics evolve weekly. Almost no weapon … that we once supported Ukraine with, is today used in the same way as it was intended to be used."[57] Russia has also embraced the need for constant drone innovation with its establishment of the Rubicon Center for Advanced Unmanned Technologies. Rubicon is aimed at rapid adaptation by assigning operators, engineers, technicians, and specialists to the same unit, allowing collaboration at a much faster pace than if they were physically separated.[58]

sUAV that routinely fly through radar blind spots or that use terrain masking. sUAV airspeeds can spoil detection, as their slow speed makes them difficult to differentiate from birds or other wildlife.[17] As the Estonian Minister of Defense stated when describing drone operations in Ukraine, "Detection—especially detection on the low altitudes—this is the most difficult part and when you add to the drones, the low-flying cruise missiles, then the detection is really a challenge."[18] Together, these properties make early detection of sUAV especially challenging and highlight the need for long-range sensors or networks of sensors optimized for sUAV detection.

The ease and rapid pace with which sUAV can be modified enables militaries to outpace efforts to develop defenses. The unmatched flexibility to quickly adapt sUAV to changing electronic jamming and electronic countermeasures has improved drone survivability. Antennas and receivers can easily be added or removed, and software can easily be changed on the battlefield to overcome adversary jammers. The Ukrainians have demonstrated the flexibility inherent in sUAV by continually surveying the RF spectrum, analyzing the data while searching for exploitable gaps, and then adapting to their findings on the fly.[19] The Ukrainians also equip some sUAV with multiple receivers and multiple antennas operating on different polarities to increase the chances of maintaining a secure datalink even in heavy electronic warfare (EW) environments.[20] The dynamic RF environment requires this perpetual, competitive adaptation cycle, as the Russians are also continuously modifying their own posture. Any military must anticipate a similar adaptation cycle when it comes to sUAV. This move-countermove style of warfare is an unending game of cat and mouse in which each side evolves based on the moves of the other. The side that can develop effective countermeasures and modify its equipment at a faster pace gains the advantage.

Evolving sUAV control methods frustrate defensive efforts

sUAV can be controlled through a multitude of methods, constituting another complication to defending against these threats. The rapid evolution of RF to fiber-optic control is just one example of how control methods seek to exploit seams in sUAV defenses in the Russian–Ukrainian War. For example, Ukrainian FPV drones used RF datalinks when they were introduced on the battlefield. As their use spread, drone operators were forced to use fiber optic cables to counter RF

Figure 2: AWACS aircraft destroyed by Iranian missile/drone attack in March 2026 at Prince Sultan Air Base, Saudi Arabia.

Photo from [Air Force ANM/NCO/SNCO Facebook]

jamming and interference. Fiber-optic sUAV have a regular operational range of 10 km, but technological advances have increased this range up to 40 km.[21] Both the Russians and the Ukrainians have also exploited civilian infrastructure, employing commercial cell phone data networks to enable control of drones deep into each other's territory. Other drones reduce dependence on precision timing and navigation signals (PNT) such as GPS by integrating cameras with terrain recognition software supported by artificial intelligence (AI) algorithms.[22] These numerous methods of control make defense difficult and encourage a system-of-systems approach to detect and stop as many of these threats as possible.

Fighting forces, using these innovative tactics, can build strategies that increase target base vulnerabilities and harness the element of surprise. The Department of Defense's Strategy for Countering Unmanned Systems states, "From the Middle East to Ukraine and across the globe—including in the U.S. homeland—unmanned systems are reshaping tactics, techniques, and procedures; challenging established operational principles; and condensing military innovation cycles."[23] Operations Spider Web and Rising Lion each demonstrated novel combat applications combining beyond-line-of-sight sUAV with special operations (SO) ground elements. In Operation Spider Web, Ukrainian operatives forward-located hundreds of quadcopter sUAV armed with small explosives deep into Russian territory. They then launched swarms of quadcopters from trucks to strike long-range Russian strategic aircraft parked on the ground using civilian 4G and LTE telecommunications networks.[24] Israeli SO ground elements also employed sUAV deep in enemy territory during Rising Lion to target Iranian C2 facilities, overwhelming air defenses and disrupting military kill chains.[25] These two operations illustrate how sUAV, controlled by beyond-line-of-sight C2 datalinks, could have a long-range strategic impact on the battlefield. They also reveal how the aircraft's small size affords flexibility for covert transport to launch areas far beyond the conflict's front lines. Launch points in proximity to air bases significantly reduces the time available to respond to inbound threats. Aircraft launched from non-fixed sites further complicate established defensive constructs, introducing an unpredictable element of surprise.

Adequate air base defense requires that future systems not only be interoperable, but also easily modified to counter an evolving threat. Battlefield innovation is a hallmark of sUAV, particularly as their low cost and ease of modification lend themselves to constant evolution. In just a few years, the Russians and Ukrainians have revolutionized nearly every aspect of sUAV employment. The list of modifications is long: C2 signals, antenna diversity, fiber-optic control, air-to-ground weapons, air-to-air weapons, the use of LTE cell phone networks for C2, the use of sUAV as interceptors, employment doctrine, and rapid software updates all top the list. These modifications highlight the need for counter–UAV systems that are similarly flexible. Systems responding to sUAV must mirror the threat they address—they must have the ability to quickly evolve (both in hardware and software) to cope with the constantly evolving threat.

Existing air base defense is insufficient against sUAV attack

The U.S. Army has historically been tasked with a fundamental role in the air defense of air bases, but its current defensive capabilities and capacity are not proving adequate given the scale and scope of the threat, especially when considering new counter–sUAV requirements. A 2020 RAND report focused on U.S. Army air base defense and concluded that the service's prioritization of other tasks and functions over air base defense resulted in a failure to meet U.S. Air Force needs.[26] Twenty-five years of unquestioned air superiority in desert warfare have made the U.S. Army complacent. It is not adequately defending air bases, and this places Airmen, air bases, and critical U.S. Air Force assets such as combat aircraft and munitions at an increasingly significant risk. The March 27 destruction of the E-3 AWACS and injury of over ten U.S. service members serves as a warning of what can happen if the responsibility for air base defense is not sufficiently prioritized with a layered set of capabilities.

In the current defensive paradigm, the U.S. Army Air and Missile Defense Command (USASMDC) provides the requisite point defense capabilities against modern aircraft and ballistic missiles for forward-deployed air bases across the Central Command theater of operations. For years, soldiers have, at least in doctrine, been tasked with executing the kill chain—detect, track, identify, and engage—against traditional ballistic missile and aircraft threats. This traditional mission still matters and must remain a priority. However, the sUAV threat does not fall into traditional threat matrices. New solutions are required.

Tower 22

The fatal attack at Tower 22 in Jordan illustrates how every second counts when identifying sUAV threats and the importance of realistic exercises. The defenses of Tower 22 failed when soldiers in the BDOC did not properly monitor the facility's air defense systems. The base's radar systems detected inbound sUAV, but the soldiers did not identify the radar tracks as viable threats prior to the successful attack.[59] Their inaction resulted in the deaths of three soldiers and injuries to another 70. The U.S. Army's investigation into the attack identified several lessons from the tragedy. First, the soldiers responsible for base defense had been distracted by the return of a friendly sUAV. The distraction caused the soldiers to miss the inbound threat and allowed it to strike without warning. Had the soldiers recognized the threat, they could have directed the base's soldiers to take immediate cover. Even a couple of minutes could have made a difference. Second, the report found that the battle drill exercises used to train and prepare for these threats were inadequate.[60] Given that sUAV can travel at hundreds of miles per hour and that their detection can be delayed due to their low flight profiles, response times can be short. BDOC personnel must clearly understand their responsibilities to operate under pressure and under tight time constraints, or the results can be deadly. Realistic exercises help ensure these critical personnel can perform their duties while stressed and when needed.

Desired effects	Capabilities currently in use or under development
Detect slow speed and small size targets	Wisp* (passive IR detection and tracking) Spark (dual-band, hemispheric radar sensor with advanced signal processing)
Detect RF usage	KuRFS (Ku-band Radio Frequency Sensor—360-degree, active electronically scanned array (AESA) radar; part of LIDS (Low, Slow, Small Unmanned Aircraft Integrated Defeat System) Spyglass (algorithmic enhanced Ku-band phased array radar)
Deliver constant, autonomous surveillance	Sentry (autonomous surveillance using AI to detect, identify, and track potential targets) Wisp (passive IR detection and tracking)
Destroy drone swarms	Coyote Block 3NK (low-cost, rail-launched missile with a boost rocket motor and a turbine engine) Mjölnir** (advanced HPM weapon system)
Identify and block adversary EM frequencies Disrupt drone communication and GPS	EM-Vis Deceive (dismounted modular electromagnetic attack (EA) system) DroneGun (multi-frequency RF disruptor anti-drone gun)
Intercept drones at low cost	Merops (mobile, AI-enabled fixed-wing effector), Roadrunner (VTOL autonomous effector), Coyote (low-cost, rail-launched effector)

Table 3: Sample C-sUAV capabilities & publicly known technologies.

*In March 2026, the U.S. Army awarded an up to $20 billion contract to Anduril involving the technology listed here.[61]

**The Air Force Research Laboratory awarded a contract for this weapon system, based on its earlier THOR, to Leidos in 2022.[62]

Traditionally, the U.S. Army has relied on four pillars to defend air bases: 1. professional and properly trained soldiers; 2. an effective C2 system; 3. technologically advanced radars; and 4. effective interceptor missiles. The U.S. Army has honed these pillars—the people, employment, and technology—into one that is optimized against manned aircraft and ballistic missiles, but it is not well aligned for the C-sUAV mission. Many of the U.S. Army's advanced missile tracking radars are not effective against sUAV because of their small size and low-altitude flight profiles. The U.S. Army's missiles (e.g., Patriot missiles) are also ineffective against the smaller and slower sUAV. The Patriots are designed to intercept high-speed targets with sufficient mass to permit effective warhead fusing. The physical characteristics of quadcopters make them poor targets. And although Patriot missiles might successfully intercept Shahed-class sUAV, the cost differential makes this prohibitive at scale. Therefore, sensors tailored to detect and track sUAV must be acquired and linked to effectors able to intercept and destroy the wide range of sUAV likely to be faced by Airmen.

Table 3 provides some of the capabilities sensors and effectors must have to successfully complete the kill chain against sUAV, along with publicly known example technology addressing some (but not all) of these issues. As small physical size limits the effectiveness of typical radars, sensors that use infrared or multi-radar bands have demonstrated improved capabilities against sUAV. Many sUAV are controlled using a datalink transmitted across radio frequencies. Detection of these RF signals can often be the first indication that sUAV are operating nearby with advanced technologies capable of triangulating sUAV position from the RF emissions. Drone swarms are difficult to defend due to their massed effects. Non-kinetic high-powered microware emitters provide the ability to simultaneously disable a large number of drones within proximity. Other defensive

Vulnerability of Land-based Air Defense Radar

Land-based air defense radars are high-value targets and, consequently, often one of the highest priority targets for an adversary. Recent combat operations in the Middle East highlight difficulties defending these types of radars. On March 24, 2026, at Victory Base in Iraq, for example, an Iranian small UAV destroyed an AN/MPQ-64 Sentinel radar, a system used to close the kill chain for the short-range air defense (SHORAD) system.[63] That same month, in Jordan, Iran destroyed an AN/TPY-2 radar, significantly degrading U.S. air defense capabilities in the region.[64] Redundant radar systems on the ground and in the air would reduce base defense single points of failure and significantly improve defensive postures.

systems disrupt the signals used by sUAV for navigation or aircraft control, rendering them ineffective. Finally, one of the most promising C-sUAV technologies is the drone interceptor. It is an sUAV designed to physically run into threat sUAV, causing both to crash into the ground. These have demonstrated exceptional effectiveness in modern combat operations.

Given the scale and severity of the sUAV threat, as well as the fact that the U.S. Army is ill-equipped to defend air bases against sUAV, there is a real risk that USAF air bases could be rendered incapable of generating combat sorties and therefore neutralized. Generating airpower is the core mission of the service. The USAF must, consequently, assume primary responsibility for defending air bases. Furthermore, only Airmen have the unique skillsets and battlespace conceptualizations—embodied in counterair doctrine and offense-as-defense mindset—required to defeat sUAV at an operationally relevant speed and scale. This is an additive mission. The U.S. Air Force must adapt C-sUAV operations in a manner aligned with counterair doctrine.

Reconceptualizing Air Base Defense for sUAV

Effectively countering the sUAV threat requires layered point defenses at each air base, a combination of offensive and defensive counterair efforts, and the integration of _tection postures into air base flightline operations to further improve force protection.

Layered point defenses are not just about fielding more kit: They also require properly trained Airmen who understand the spectrum of threats, can plan air base defense accordingly, and can operate the various defensive systems used in base defense. Part of this is implementing passive base defense measures. A layered defense means effective C2 systems centered on the U.S. Air Force's base defense operations center; the acquisition and deployment of interoperable equipment for airborne early warning, tracking, and identification; and the fielding of capabilities that can then defeat airborne threats. To complement these defensive counterair efforts, offensive counterair efforts include all measures that seek to defeat enemy strikes before they can occur. This includes targeting adversary factories, storage facilities, and C2 nodes and networks. Finally, a drone protection posture can bridge the gaps left by more traditional base defenses. Implementing tiered readiness levels based on immediate or impending sUAV threats can help warfighters prepare for these new threats. Engaging in routine exercises to ensure timely air base–wide C2 is also fundamental. Through reps and sets, Airmen gain a clear understanding of required actions within each posture.

The foundation of an sUAV base defense starts with layered point defense. Numerous holes in the existing base point defense architecture necessitate an overhaul to achieve even a basic level of base protection. First, extensive training is required. Airmen require training to plan air base defense and to operate the systems used to defend the base.

The U.S. Navy's Billion Dollar Defense

The U.S. Navy's experience in the Red Sea against the Houthis is a clear example of just how expensive current C-sUAV tools are. U.S. Navy defensive actions demonstrated high levels of success but at a massive economic cost. Using a layered air defense network of intercept aircraft, various surface-to-air missiles, short-range surface-to-air guns, and a suite of electronic attack options, the U.S. Navy intercepted an estimated 480 Houthi attacks by missiles and drones. This successful defense was incredibly resource-intensive, requiring hundreds of surface-to-air missiles, hundreds of rounds from surface-to-air guns, and a total cost of over a billion dollars.[65] These high costs have caught the attention of senior military leaders, with Vice Chief of Naval Operations Admiral James Kilby noting, "The Navy's current reliance on high-cost interceptors, such as SM-6 and SM-3, is unsustainable in high-tempo operations."[66] Moving forward, the military must shift to lower-cost and more plentiful alternatives when dealing with the prolific small UAV threat.

Next, the BDOC must be modified. Timely information must inform air battle experts of air threats to the base, and these personnel must be empowered to direct proper base response. Bases require layered multi-spectral sensors capable of detecting and defeating large numbers of adversary sUAV. Finally, point defense requires the implementation of passive base defense measures that mitigate sUAV attacks able to circumvent defensive constructs.

However necessary point defenses are, they are insufficient on their own. The volume of sUAV threats observed on modern battlefields requires deliberate efforts to stop as many of them as possible before launch. The targeted destruction of factories, storage facilities, C2 nodes, and logistical supply lines all reduce the number of sUAS threats and improve overall air base security.

The final component of sUAV defense is the revival of a base's ability to survive and operate while facing a constant threat. For years, Airmen have accomplished their expeditionary mission of generating combat airpower with little concern for an air threat. sUAV change this calculus. Each member of an expeditionary air base must understand the threat, stand vigilant for the threat, receive real-time threat updates, and become adept with the equipment and procedures needed to properly balance force protection with mission accomplishment. This will come in the form of tiered protection postures based on the sUAV threat.

Generating a defensive plan

As a first step in response to the emerging sUAV threat, Airmen must build a defensive plan. Effective air base defense against sUAV requires deliberately designed, layered, and integrated operations that combine detection, tracking, identification, engagement, and defeat. This entails fusing sensors, intelligence, and C2 to enable timely decisions based on clear engagement authorities. Effective plans must account for the engagement cost, volume, and rapid innovation cycles of sUAV by incorporating EW, kinetic and non-kinetic options, and passive defenses such as camouflage and dispersion. Ultimately, successful defense depends on effective training, exercises, and seamless coordination across security forces, air defense, and aviation units to protect aircraft and personnel while maximizing mission continuity. Successfully integrating and employing all these sUAV defensive components demands an effective C2 system or a BDOC prepared to engage this new class of threats.

Reconceptualizing the BDOC for the counter–sUAV mission

U.S. Air Force leadership must transform the BDOC into an air base C2 hub capable of responding to the dynamic UAV threat.

Because the current BDOC construct is part of the USAF base's security forces, it serves as the tactical nerve center for most U.S. Air Force bases and has traditionally focused on ground security, not air threats. BDOC controllers monitor all security and law enforcement operations with security cameras, radios, and patrols across the installation. A revamped BDOC must broaden its attention and situational awareness to include air threats. Most importantly, the BDOC must develop the capacity to execute the kill chain in a timely manner against the robust and ever-changing sUAV air threat. This will require incorporating an airborne common operating picture into daily operations. Above all, the reconstructed BDOC must constantly assess the threat environment and take appropriate actions to warn the base of and mitigate an attack.

The Airmen staffing the BDOC currently lack necessary skills and require additional training to take on the responsibility for air defense. USAF leaders are increasingly aware of this shortfall. U.S. Air Forces Central Command (AFCENT) has assigned a group to focus on counter–sUAV challenges to better defend Airmen at deployed locations.[27] The AFCENT team recognized that because the Airmen manning the BDOC traditionally come from security forces and do not possess the skills needed to perform air defense operations, they also lacked key competencies to conduct C-sUAV operations. Specifically, the AFCENT team identified the need for BDOC manning to include air battle managers (ABM) and weapons directors (WD), both specialties that typically fill important roles on airborne early warning aircraft (AWACS) or in land-based control and reporting centers (CRC). ABMs and WDs understand airspace control, three-dimensional airspace, threat-identification matrices, and intercept geometry. Any future air base C2 center will require these skills. In response to the need for appropriately trained base defense Airmen, the U.S. Air Force recently announced the creation of "Point Defense Flights" at select bases and the creation of a new enlisted U.S. Air Force career field trained to defend bases from aerial attack.[28] Details pertaining to the career field are forthcoming.

Transforming the BDOC into an effective air base defense C2 node will require tying airspace awareness, C2, and employment together. The BDOC must become the nerve center responsible for the timely execution of the kill chain against incoming threats. Airmen equipped with the skills of ABMs and WDs must accomplish each step of the kill chain under tight time constraints to protect the air base and its valuable assets. The BDOC must also be equipped with the appropriate technologies to expeditiously execute the kill chain—the ability to detect, track, identify, and defeat inbound threats.

Defensive operations in Ukraine demonstrate the importance of detecting sUAV early, because the greater the amount of response time, the greater the number of potential responses. Where 30 minutes might afford the deliberate massing of effects against inbound sUAV, 3 minutes might barely provide enough time to take cover. The threat of large numbers of sUAV—employed as a swarm toward a single target or launched en masse at numerous targets—also highlights the importance of early detection. To gain this critical response time against large swarms of sUAV, Ukrainian forces have placed their sensors hundreds of miles beyond their air base boundaries, creating a "defense-in-depth" against sUAV. The success of these defense-in-depth systems highlights that effective kill chain execution requires seamless integration of highly trained personnel, layered sensors, effective interceptors, and a C2 system tying it all together. The early detection often permits an intercept by Ukrainian F-16 fighter jets or Merops-interceptor sUAV.[29] Deploying these waves of interceptors increases the probability of neutralizing large numbers of sUAV. And if threat interception is unsuccessful, early detection permits maximum response time to seek cover. The greater the amount of time provided to respond, the better the chances of mitigating the threat.

Knowing who or what to kill: identification of friend or foe

The timely labeling of friend or foe is an essential element in any threat response and is naturally included in an sUAV combat ID matrix. The addition of manned/unmanned labels to existing combat ID matrices would improve an air base's ability to defend itself while potentially reducing the risk of accidental fratricide of friendly manned aircraft. Large numbers of threats require more time to respond. The fog and friction of combat sometimes drive decision-making based on incomplete information. Faced with a high-speed inbound air threat and absent of resolute hostile declaration, a decision-maker could still engage the potential threat free of concern for human casualties if they simply knew it was an unmanned aircraft. Adding an unmanned identification label to inbound threats allows the defender to engage under time-constrained situations with incomplete target identification and minimize the chance of accidently killing friendly aircrew. As the numbers of airborne tracks continue to increase, tagging tracks as manned/unmanned is an easy initial measure that strengthens base defense.

Whether an aircraft is manned or unmanned is of utmost importance in 21st-century combat, and modifying the combat ID matrix to account for this status allows engagement authorities to better balance risk when defending air bases. On this issue, lethal autonomous weapon systems (LAWS) continue to garner greater attention as technology matures, with some observers concerned that killer robots could roam the battlespace, autonomously killing people. The DOD/W has defined LAWS as "weapon system[s] that, once activated, can select and engage targets without further intervention by a human operator."[30] This concept of autonomy is also known as "human out-of-the-loop" or "full autonomy," but as of early 2026, DODD 3000.09 requires that all systems, including LAWS, be designed to "allow commanders and operators to exercise appropriate levels of human judgment over the use of force."[31] The U.S. Navy's AEGIS air defense combat system has already demonstrated the combat success of automated systems. In many defensive scenarios, actions taken by the AEGIS system occur at speeds where there's no time for the operator to be in the loop.[32] As the battlespace is populated with greater numbers of unmanned aircraft massed with ballistic and cruise missile salvos, fully autonomous systems may be required to defeat the threat. Whether an aircraft is manned is an important piece of the risk calculus governing engagement and should be included in the combat identification (CID) matrix. It is reasonable to assume the need for stricter oversight of force when human lives hang in the balance. CID plays a foundational role in the rules of engagement, and the proliferation of unmanned aircraft demands this fundamental change.

Freedom of Action

"Freedom of action in the electromagnetic spectrum, at the time, place, and parameters of our choosing, is a required precursor to the successful conduct of operations in all domains. Forces in 2030 and beyond will be ready to fight and win through the deliberate, institutional pursuit of EMS superiority." —Department of Defense, Electromagnetic Spectrum Superiority Strategy, October 2020[67]

System type	Sensor type	Strengths	Weaknesses	Example system
Ground-Based Radar	Active	Long-range detection, wide-area surveillance	Vulnerable to attack, limited low-altitude effectiveness	AN/TPS-80, Long-Range Persistent Surveillance
Airborne Radar	Active	Long-range detection, wide-area surveillance	Limited low-altitude effectiveness, expensive to fly 24/7, high power requirement	E-7 Wedgetail, MQ-9
Acoustic	Passive	Inexpensive, low power requirement	Short-range, low resolution, susceptible to sound pollution	Doscoviar G2
Radio Frequency	Passive	Difficult to detect, multiple targets tracking	Ineffective against non-transmitting systems, requires RF catalog of signals	Tsukorok, X-MADIS
Optical	Passive	Difficult to detect, low power requirement, visual target identification	Short range, line-of-sight dependency, susceptible to adverse weather	Night Hawk HD

Table 4: Potential sensors, radars, and other detection systems to be included in a defense-in-depth C-sUAV approach.[68]

Detecting & defeating the swarm

Air bases require weapon systems capable of detecting and intercepting large numbers of sUAV in short periods of time. The unique characteristics of sUAV—low-altitude flight paths, wide-ranging airspeeds, small physical profiles, and non-traditional material compositions—mean that current air defense systems struggle to initiate and close kill chains against them. Of the very few counter–sUAV systems across the U.S. Air Force, most are deployed to expeditionary overseas bases. The majority of domestic air bases lack C-sUAV systems entirely.

The USAF must field integrated systems capable of detecting, tracking, identifying, and defeating sUAV threats. Ideally, these systems would be situated across vast distances, creating a defense-in-depth that increases the time available to complete the kill chain. Defending and defeating enemy sUAV begins with a layered mix of RF sensors, radars, and acoustic and electro-optical/infrared systems tied to data fusion tools that feed into a common operating picture. Fielding and fusing diverse sets of sensors can maximize detection time and minimize coverage gaps against the various types of small UAV. This integrated set of sensors provides pertinent data to detect, track, and identify threats approaching an air base. Table 4 presents a sample of sensors, radars, and other detection systems that could be integrated into an effective defense-in-depth C-sUAV approach.

Operational limitations of land-based sensors make airborne sensors a compelling additional component to detect, track, and identify sUAV. Land sensors have very limited effective ranges against low-altitude targets due to obstacle masking. Fixed radar sites have lost their efficacy throughout the Ukrainian conflict, with both Russian and Ukrainian sUAV operators learning to avoid overflight of ground radars, delaying the detection of inbound threats.

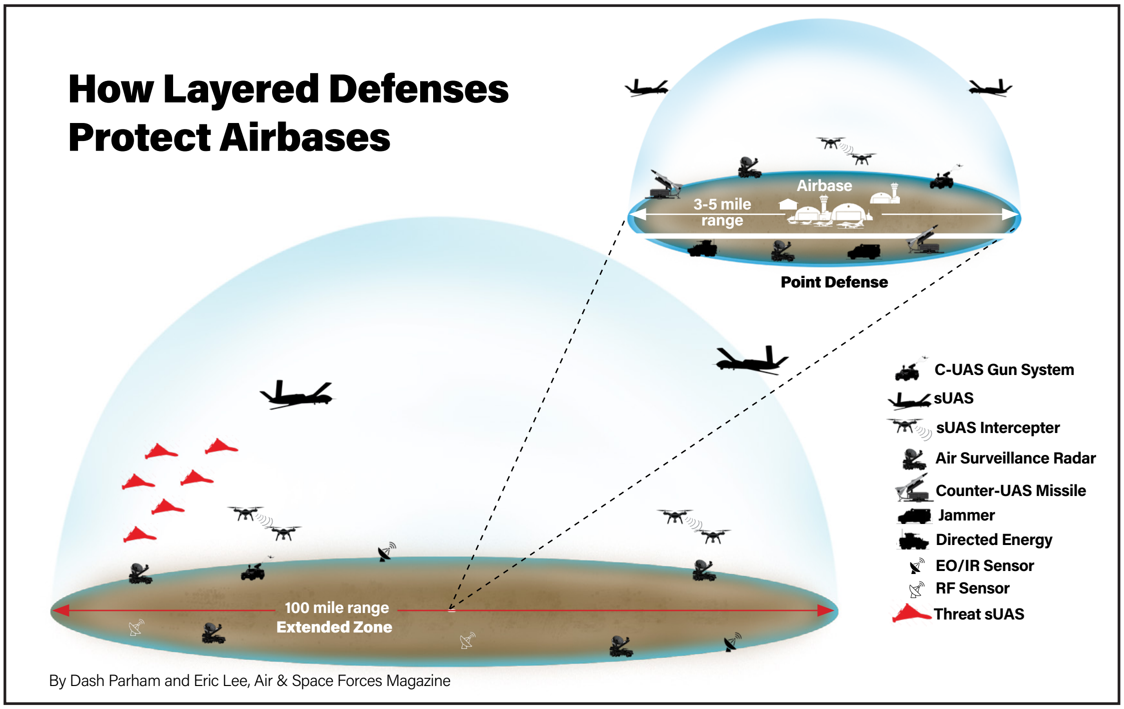

Figure 3: Theoretical layered air base sUAV defense network.

A promising approach is to turn to long-endurance airborne sensors like those found on AWACS aircraft. These sensors do not stay in a fixed position, so adversaries cannot learn their location to avoid them. Specialized sUAV airborne sensors can also be integrated with medium/high-altitude long-endurance drones like the RQ-4 Global Hawk and the MQ-9 Reaper.[33] In areas of low air threats, these aircraft can advance forward in the battlespace to provide early warning of inbound small UAV threats. Airborne sensors also greatly reduce the impact of terrain-masking, further improving their effectiveness. Airborne sensors improve situational awareness across the battlefield, making them an important early warning capability against sUAV.

Finally, airborne sensors can respond to real-time intelligence and focus on expected attack vectors from specific locations, permitting the ability to concentrate effort—a benefit not available from fixed assets. But airborne sensors bring limitations. They are extremely constrained in numbers. Existing U.S. Air Force UAV require deliberate research and development efforts to make them viable early warning platforms that can overcome difficult sensing challenges such as ground clutter and slow-moving sUAV. Despite these limitations, synthesizing airborne sensors with a robust ground network improves overall detection capabilities and remains a key component of sUAV early warning.

The varied physical characteristics of small UAV, combined with their diverse C2 means, make multi-spectral and layered sensor networks—both ground and air—a requirement for air base defense. Several systems already exist that can detect, track, and identify sUAV, including the U.S. Army's Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System (M-LIDS) or the U.S. Air Force's Small Unmanned Aircraft Defense System (SUADS). These systems remain under development and highlight the challenge of integrating multiple types of sensors into a single system. Combat operations in Ukraine continue to demonstrate the importance of

System	Strength	Weakness	Commercial examples
Laser	Low cost-per-engagement, deep magazine	Dependent on maintaining precise target track, dust/smoke reduces effective range, short range	Locust X3, H4
High-Power Microwave	Able to engage multiple sUAV simultaneously, low cost-per-engagement, deep magazine	Short range	Leonidas
RF Jammer	Low cost, low collateral damage	Short range, ineffective against sUAV flying direct to coordinates	Pulsar, Dobermann
Surface-to-air gun	Low cost	Difficult to guide accurately	C-RAM
Surface-to-air missile	High probability of kill,	High cost, limited magazine depth	SM-3
Drone Interceptor	Low cost, long range	Dependent on precise guidance throughout intercept	Sting, Anvil

Table 5: Comparison of various effector types currently commercially available.

multi-spectral and layered employment of sensors, including radar, audio, IR, and RF. Each sensor type brings inherent strengths and weaknesses against the various types of sUAV threats. Where a low-altitude small first-person view (FPV) quadcopter might avoid radar, it certainly could be discovered by an RF detector, such as AeroVironment's Titan System. The U.S. Air Force at Grand Forks AFB's Point Defense C-UAV Battle Lab is currently testing these systems. Long-range Shahed attack drones would be detected by traditional radar when flying at 10,000 ft, but they might not be at lower altitudes. However, low-altitude sUAV are loud and can be detected by audio sensors, which have had surprisingly good results defending Ukraine.[34]

The tremendous diversity of small UAV threats is yet another level of complication to detecting and defeating them. No single defensive system can address all the different signatures, flight profiles, and attack methods presented by these threats. Instead, defenders must integrate multiple effectors—kinetic, EW, and directed energy—across overlapping engagement zones to create depth and resilience. Table 5 lists examples of current effector types, including their costs, strengths, and weaknesses. The ideal effector is not universal; it depends on many factors, including expected threat, collateral damage concerns, surrounding proximity, weather, effector placement, and size of area defended. This approach enables forces to match the most appropriate effector to each target while preserving high-end capabilities for more complex threats. Adapting the BDOC for C-sUAV would be essential to prioritizing these defensive responses. A layered system could also mitigate saturation attacks and cost-imposition challenges by combining low-cost, high-volume solutions with more advanced interceptors across a defense-in-depth system. Ultimately, effective counter–sUAV requires a system-of-systems approach that combines layered sensors with a diverse set of effectors into a coherent defensive network commanded by the BDOC.

The rockets and drone interceptors pictured in Figure 4 are two capabilities that are already demonstrating exceptional combat effectiveness at negating the sUAV threat at a reasonable cost. Both the United

Figure 4: Two promising cost-effective C-sUAV effectors are AGR-20F Advanced Precision Kill Weapon System II laser-guided rockets, loaded on either F-15E Strike Eagles or MQ-9 Reapers, and Anvil drone interceptors.

Credit: U.S. Air Force Courtesy Photo; MQ-9 courtesy of General Atomics Aeronautical; Anvil courtesy of Anduril Industries.

States and Ukraine have effectively employed the Advanced Precision Kill Weapon System (APKWS) rockets. These rockets cost roughly $25,000 per shot, making them an excellent option when considering cost-exchange ratios in a mass-sUAV attack.[35] Combat proven on both the F-16 and F-15E fighter aircraft, APKWS rockets have also been successfully tested on MQ-9 aircraft, which can provide much greater battlefield persistence than fighter aircraft.[36] In addition to the rockets, Ukraine has significantly increased the fielding of drone interceptors with positive battlefield results. Although Russian drone and missile attacks have grown to over 6,000 per month, Ukraine defeats 90 percent of the threats using drone interceptors.[37] These relatively inexpensive Ukrainian drones fly around 200 mph, cost between $1,000–$2,500, and combine IR, radar, AI, and manual human controls to complete intercepts.[38] As with every sUAV weapon being used in Ukraine, these interceptor drones continue to evolve with new datalinks, warheads, and sensors.

The United States already possesses several weapon systems capable of intercepting sUAV, even in a layered air-defense network like that proposed in the figure above. However, as the U.S. Navy experienced in the Red Sea against the Houthis, these current weapon systems are incredibly expensive. The low cost and large numbers of small UAV require counter-systems that factor cost-per-effect into the calculation. Simply put, many of the weapons currently used by the United States to intercept sUAV are an order of magnitude more expensive than the drones they are destroying. This puts the United States at the losing end of the cost-exchange ratio, risking the U.S. Air Force's ability to procure enough counter–sUAV systems.

Drone-targeting interceptor	Cost per interceptor (million USD)
SM-3 Block IIA	~$27.9M
SM-3 Block IB	~$9.7M–12,5M
SM-6	~$9.6M
THAAD Interceptor	~$12–13M
Patriot PAC-3	~$3.7M
Stinger	~$500K

Table 6: Current common (and expensive) drone-targeting response technologies.[70]

As the military services acquire sUAV defensive systems, standardized data sharing is imperative to permit the creation of a joint common operating picture. The DOD/W created the Joint Interagency Task Force (JIATF) 401 for just this reason. JIATF 401 leads the Pentagon's counter–UAV efforts and is tasked with standardizing C-UAV across the services. In early 2026, JIATF 401 inked a first-of-its-kind common data protocol standard for C-UAV technologies with the United Kingdom, not only to standardize data sharing within the United States but also to push for the same internationally.[39] The U.S. Air Force is currently developing the SUADS with the company Trust Automation to detect, track, ID, and defeat sUAV; however, little is publicly known about the system's details or its efficacy.[40] SUADS purports to bring all the pieces together—sensors, effectors, and C2—to close the sUAV kill chain. With this objective in mind, future versions of U.S. Air Force SUADS must use standard data protocols, permitting integration with sister-service systems.

Passive defensive measures are key to resilient base operations

The integration of passive measures is also essential to defend air bases against sUAV, particularly in the event the threat penetrates the defensive perimeter. As evidenced in modern warfare—and as the Russian tactics of sUAV swarming in Ukraine have illustrated—some sUAV will penetrate an air base's defenses, leaving only passive defensive measures to mitigate the effects. Traditional camouflage and deception efforts, for example, can prevent adversary sUAV from finding their intended targets. Dispersion likewise makes it more difficult for the enemy to locate important targets, as assets can potentially be relocated faster than satellite revisit rates. This can also limit the spread of damage even if some targets are hit. In addition, the hardening of infrastructure and aircraft shelters protects valuable assets even when sUAV locate their target. Finally, the new concept of "emplacement"—the intentional fielding of barriers meant to intercept or preclude sUAV from reaching their targets—has shown tremendous potential in the Ukrainian battlespace. Ukraine's extensive use of netting is an excellent example of emplacement reducing the effectiveness of sUAV attacks. These barriers are low-cost and have little impact on the storage and generation of aircraft. Passive measures have demonstrated real-world effectiveness at reducing the effects of sUAV attacks, but they require prior planning and implementation to be effective.

Sustained Air Base Defense Requires Offensive Counterair Efforts

WWII demonstrated the importance of combining defensive and offensive counterair efforts to achieve dominance in the air and, consequently, success across domains. Counterair operations aim to prevent prohibitive interference to friendly forces from the enemy in the air domain. Historically, this required a combination of offensive and defensive counterair operations. The prolonged WWII air war over Europe demonstrated the importance of these combined efforts, with the campaign against the German Luftwaffe establishing the principles of an offensive counterair campaign. Offense was used defensively to forestall attacks. Aircraft factories; airfields; ball-bearing factories; petroleum, oil, and lubricant factories; and storage were attacked to reduce the number of Axis aircraft that could, in turn, attack Allied forces. Defensive counterair efforts were widespread throughout the war as well, the most famous being the Battle of Britain, where aircraft patrolled the skies over England. Furthermore, an elaborate set of radar sites—Chain Home—enabled timely execution of the kill chain's detect, track, and identify stages. This same construct of offense combined with defense must be applied when defending against sUAV.

The application of this counterair doctrine construct still proves out in Ukraine and Iran in 2026. Both Russian and Ukrainian forces have demonstrated the importance of offensive operations in any counter–sUAV strategy: Both have already preemptively launched missions targeting each other's sUAV pilots and the infrastructure involved in producing sUAV. Drone pilots, in particular, have been high priorities, with some Russian fighters describing Ukrainian drone pilots as "target No.1."[41] Ukraine, in an operation dubbed "Dronocide," cataloged Russian sUAV operating locations along the Orikhiv front and then orchestrated an attack on 46 separate locations specifically targeting drone operators.[42] Ukraine also deliberately attacked a number of facilities required for the production and operation of long-range drones. As just one example, Ukrainian forces targeted Russian factories responsible for the production of thousands of strike and reconnaissance drones in January 2026. The Ukrainians have successfully targeted logistics hubs and oil refineries, all with ties to the vast Russian drone enterprise. In describing the early results of Operation Epic Fury, Chairman of the Joint Chiefs of Staff Gen. Dan Caine reported, "Perhaps most importantly, we've destroyed Iran's defense industrial base and their ability to reconstitute those capabilities for years to come. We attacked, along with our partners, approximately 90 percent of their weapons factories … Every factory that produced Shahed one-way attack drones was struck. Every factory that produces the guidance systems that go into those drones was struck."[43] Destruction of these facilities not only slows production output but also forces logistical dispersion and raises the adversary's costs of sustaining combat operations.

Targeting UAV production facilities, supply chains, & warehouses

Stopping or reducing the production rates of sUAV is essential to decreasing the overall sUAV threat. This can be accomplished by targeting any of a series of steps that comprise the manufacturing process. sUAV production depends on a host of key components: batteries, brushless motors, and small turbine engines, to name a few. Ukrainian forces have already proven that targeting and destroying the aircraft factories themselves slows production; targeting the warehouses storing these components could potentially achieve the same result.[44]

The scale and depth of sUAV logistics mean that the destruction of any of a wide variety of potential targets could substantially reduce an adversary's ability to sustain these operations. In fact, achieving this effect was an explicit aim of the United States' Operation Epic Fury in Iran. The large number of these small aircraft results in a sizeable ground footprint. Factories, large warehouses, and launch sites have been seen housing hundreds of Shahed-sized sUAV.

It is true that the stockpiling of Type 1 quadcopter UAV smaller than the Shaheds has typically not been observed. It simply does not make tactical sense to store large numbers of these small quadcopter UAV in warehouses, given their high combat expenditure rates and rapid technological obsolescence. While these types may not have targetable storage, the factories or the supply chain of parts required for their mass production offer lucrative targets to reduce their overall numbers across the battlespace. Despite the rapid innovation cycles of these types of drones, components like blades, motors, and batteries remain relatively stable. Even as their control, datalinks, and navigation modes quickly evolve, the high aircraft production rates necessary for sUAV employment require a high-output manufacturing operation and stable supply chain network dependent on large amounts of parts and components.

Targeting & attacking sUAV C2 methods, datalinks, & navigation

In another application of offensive counterair targeting, Russia, Ukraine, and the United States have attacked the electronic datalinks on which a majority of sUAV rely for C2 and navigation, degrading sUAV combat effectiveness. These efforts to completely deny datalinks are separate and distinct from tactical jamming efforts that take place in and around air bases; they can be broader in scope, extend greater distances, and affect larger areas of operation. The jamming, denial, or destruction of these datalinks degrades the adversary's ability to effectively use sUAV for any purpose.

Commanders should be aware, though, of the potential for "frequency collateral damage." Some sUAV operate on frequencies similar to those used for civilian applications, while others use civilian communications systems. Adversary use of commercial communication systems for sUAV combat operations puts these civilian systems squarely in the crosshairs of C-sUAV strategy, particularly under counterair doctrine where offensive and defensive constructs exhibit fluid, even vague boundaries. Attacking these communications networks as part of a broader C-sUAV campaign is important to consider when implementing C-sUAV spectrum operations.

Ukrainians have been observed using this approach to their advantage, co-opting Russian LTE cellular telephone networks to control their aircraft deep behind enemy lines.[45] This has been especially troublesome to the Russians, forcing them to take the unprecedented action of shutting down their own cellular LTE networks across vast sections of Russia to deny the signal to the Ukrainians.

Russian sUAV are also using commercial communications networks, including the space-based Starlink network, according to some sources.[46] Countering this network is especially problematic, as jamming the 9,000–plus satellites involved is both impractical and ineffective. Instead, Ukraine has resorted to direct consultations with SpaceX, the company that operates Starlink, to deny the valuable signals to the Russians.[47] In situations where kinetic destruction or spectrum operations are impractical, negotiations with the owners of the systems, such as Elon Musk, have successfully limited their use by adversaries, ultimately reducing sUAV threats. Future offensive counterair efforts will require a detailed understanding of the adversary's communications means and methodologies. Denying their use may require non-traditional actions and negotiations with commercial communications providers.

Ability to Survive & Operate Under sUAV Attack

Despite offensive counterair efforts combined with layered point defense, real-world combat operations demonstrate that air bases will remain vulnerable to attack. Airmen must prepare to perform their primary mission of generating aircraft while under a persistent small UAV threat. If Airmen continue to perform the mission of generating aircraft without pause, then they risk exposing themselves and their aircraft to undue risk. If they go to the other extreme by securing their aircraft in hardened aircraft shelters and retreating to bomb shelters, then they risk not accomplishing their main mission of generating airpower. A thoughtful balance between force generation and force protection is required. Successfully managing the tension between force protection and mission accomplishment begins with sound intelligence on enemy activity. This, combined with an accurate common operating picture of the current air threat, can provide the foundation for risk mitigation plans. Air bases must implement a set of tiered readiness postures based on the threat to the base; these tiers can optimize how the forces on station can balance force protection with mission accomplishment. The USAF already has a similar construct on which to build: the mission-oriented protective posture (MOPP) developed in response to the chemical/biological attack threat.

Generating airpower while under threat is essential, and the construct used to prepare for chemical-biological weapons attack may prove instructive when preparing for sUAV attack. For decades, Airmen have prepared for a chemical-biological weapons attack, developing a flexible system of tiered responses (postures) based on threat level, which balanced force protection with airpower generation. The MOPP program issues Airmen personal protective equipment (PPE), requiring the wear of very uncomfortable and hot gear during routine, week-long military exercises to practice accomplishing their normal jobs across a U.S. Air Force base while under attack from simulated chemical-biological weapons. Airmen vary their level of precaution depending on the threat, with higher MOPP levels requiring greater precautions, which typically slow overall productivity.[48] Moreover, the vast expanse of many U.S. Air Force bases means that MOPP levels often vary across a specific base. Dividing the base into sections allows a response tailored to a battle damage and threat assessment. These same principles should inform an sUAV threat matrix, tailoring preplanned response postures to inbound or expected airborne threats. Table 7 offers one potential drone protection posture) based on the MOPP model.

A DPP could also divide an air base into sectors and set threat levels depending on the presence or number of inbound or attacking sUAV. At one end of the spectrum, a low threat might call for very few defensive measures as Airmen continue to focus on accomplishing their primary jobs. An imminent threat at the high end of the spectrum might force Airmen to take more extensive precautions, thus slowing their ability to generate aircraft and detracting from accomplishing their primary job of generating airpower. One option might be employing quick-reaction forces with short-range C-sUAV weapons. Some attack scenarios might even require Airmen to completely stop performing their jobs and seek shelter, while other scenarios might direct the immediate launching of aircraft, “flushing the base” to avoid inbound threats. Mitigation measures could extend into the electromagnetic spectrum, with Airmen preemptively jamming certain bandwidths to deny access to inbound threats. Ideally, the threat is defeated. If the threat is not neutralized by any of the layers of a base defense-in-depth system, Airmen at the targeted base can still take cover or initiate other DPP measures to protect valuable assets.

	Threat Posture LOW	Threat Posture MEDIUM	Threat Posture HIGH
Personnel Actions	No actions required / PPE available	Monitor air threat Radar / wear PPE	Seek shelter / wear PPE
Aircraft Maintenance Activities	Unrestricted / consider passive defenses	Implement maximum passive base defenses	Immediately launch aircraft / aircraft move to hardened shelters
			*PPE includes Kevlar helmet and vest

Table 7: Potential C-sUAV Threat Postures

In any case, development of a DPP would require consistent training and exercises to ensure effectiveness under stressful combat situations and across a unit as complex as an air base.

Using the EM Spectrum in sUAV Flight Operations & Counter–sUAV Activities Demands Proactive Operational Management & Deconfliction

The conflict between C-sUAV systems and airfield operations in a congested EM spectrum requires planning, battlefield situational awareness, and dynamic deconfliction to ensure warfighter access to critical data and information. To manage this increasingly complicated aspect of the battlespace, air base commanders must create processes and policies to deliberately coordinate the use of the EM spectrum in and around their air bases.

Daily air base operations require the use of the EM spectrum for safe flight operations. Aircraft require access to GPS, radio communications, and datalinks to execute their missions. Air base personnel use satellite communications, Wi-Fi, cellular, and Bluetooth connectivity for everyday purposes. Aircraft operations, coordination of aircraft and munitions generation, security forces communication, and myriad functions across the facility rely on these frequencies too. As a result of all these factors, counter–sUAV systems that transmit or jam across the EM spectrum must be deconflicted from the numerous systems relied on by base personnel to accomplish their duties. However, during high sUAV threat levels, base commanders must prioritize sUAV jamming and defensive operations regardless of the risk of interference with friendly systems. These responses must not be ad hoc. Instead, base commanders should create contingency plans in advance of an attack during which C-sUAV operations will likely render mission-critical frequencies unusable. Previously coordinated DPPs could mitigate the effects of this EM conflict with preestablished responses and actions.

sUAV bring electromagnetic spectrum operations (EMSO) to the forefront of airfield operations. As sUAV operators use specific frequencies to launch and control their drones, frequency jammers become an increasingly prevalent countermeasure. All the while, air base operations rely more than ever on information passed through the EM spectrum to support their main mission of generating and launching aircraft. GPS signals, for instance, provide precision navigation and timing for aircraft preparing for flight, while traditional radios continue to provide tactical communications across an installation and between the control tower and aircraft. Add to this congestion the demands of commercial applications, and the EM spectrum rapidly becomes overwhelmed with users.[49] The situation grows even more complex when considering that different countries allocate the EM spectrum differently across civilian applications. For example, whereas the United States uses 5G networks in the 3.5 GHz band, China uses frequencies in the 5.0 GHz band in addition to the 3.5GHz band.[50] Airmen operating in foreign countries must take these differences into account when executing any sort of EMSO.

The growing pervasiveness of C-sUAV electronic jammers requires air base commanders to deliberately manage the use of the EM spectrum to avoid unintended fratricide and the degradation of air base operations. RF and microwave C-sUAV systems have already been observed creating undesired collateral damage in Ukraine. Because Russian and Ukrainian drones often operate on similar frequencies, Ukrainian soldiers have inadvertently jammed their own systems while trying to stop Russian attacks.[51] Moreover, many C-sUAV systems have broad EM spectrum coverage that spans from the high-powered microwave frequencies to more familiar RF bands. Thus, employment of certain C-sUAV systems can be indiscriminate among friendly or adversary systems. When building a layered C-sUAV defense, the U.S. Air Force should seek to create focused EMSO effects, meaning that, as base commanders employ capabilities, they also deconflict C-sUAV frequencies from friendly systems. This approach is critical, as the physical and flight attributes of sUAV make kinetic kills difficult at scale.

EM spectrum deconfliction will require a central node to maintain awareness and coordination across the base. The most appropriate entity is the BDOC, which must become the real-time C2 hub responsible for collating EM spectrum data across the base. Without this C2 nucleus, determining the root cause of degraded systems would be nearly impossible across disparate units. Centralization allows greater collective awareness of C-UAV emitters across the base during dynamic situations.

Warfighter management of the electromagnetic spectrum

Beyond the air base, the proliferation of unmanned land, sea, and air vehicles, along with the accompanying C-sUAV, also contribute to a saturated electromagnetic spectrum. The spectrum must be deliberately managed by the Joint Force Commander (JFC) to minimize fratricide and to increase the chances of overall mission success. Inadequate deconfliction efforts often render many combat systems ineffective due to interference or spectrum overload. The rapid fielding of C-sUAV systems could exacerbate these existing frictions. As a result, the JFC must ensure combat forces remain fully effective as C-sUAV systems proliferate across the battlefield. Two important Department of Defense documents provide definitive guidance on joint electromagnetic spectrum operations: the Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3320.01D, Joint Electromagnetic Spectrum Operations; and U.S. Air Force Doctrine Publication 3-85, Electromagnetic Spectrum Operations.

CJCSM 3320.01D provides exhaustive guidance on EM spectrum management but lacks testing under highly contested combat conditions. Reporting on the performance of this guidance out of Operation Epic Fury has been scant. But it aims to enable joint force commanders to achieve EMS superiority and perform battle management of electromagnetic spectrum operations.[52] It provides EMSO C2 guidance, planning, and countless coordination measures. Joint military operations must continue to operationalize EMSO management concepts like these. The continued proliferation of UAV and C-UAV systems across the battlespace makes this initiative an imperative.

Recommendations

The shocking impact of small UAV across modern battlefields has fundamentally altered the character of air base defense, exposing critical vulnerabilities in existing constructs while compressing decision timelines and increasing operational risk. Traditional air and missile threats still exist, but the scale, affordability, and adaptability of sUAV demand more than incremental improvements to legacy point defense systems. Successful defense of expeditionary air bases requires a doctrinal shift that fully integrates defensive and offensive counterair principles, supported by appropriately trained forces, modernized C2, and multi-layered detection, identification, and engagement capabilities.

Airmen must organize, train, and equip to execute the full counter–sUAV kill chain—detect, track, identify, and defeat—under increasingly complex and time-constrained conditions. This includes transforming the base defense operations center into a true air defense hub, fielding layered and multi-spectral sensor networks and integrating diverse effectors capable of addressing both cost and scale challenges. This system-of-systems approach must remain adaptable to changing threats. Equally important is the adoption of new operational constructs, such as tiered defensive postures like the proposed DPP, that enable continued airpower generation while under persistent threat.

However, robust point defense alone is insufficient. As history has demonstrated, sustained protection of air bases requires deliberate offensive counterair operations, specifically the targeting of adversary launch sites, production infrastructure, and C2 networks. At the same time, the growing reliance on the electromagnetic spectrum necessitates deliberate management and deconfliction across the air base and the battlefield.

Ultimately, success against the rapidly growing sUAV threat will depend on a system-of-systems approach that integrates doctrine, technology, training, and operational concepts into a coherent and adaptable defense. To that end, the Mitchell Institute offers the following recommendations:

1. The DOD/W and Congress must provide the USAF with additional monetary and personnel support to develop and field essential counter–sUAV technology, robust passive defenses, and new defensive postures at a level that can support expeditionary and agile combat employment concepts. As a first step, the USAF must fully resource air base point-defense systems. These newly conceived U.S. Air Force point defenses must be carefully integrated with existing U.S. Army ballistic missile defense capabilities. This, in turn, necessitates reconceptualized USAF C2 structures. The USAF must also identify, acquire, and employ a standardized set of equipment that can provide airborne early warning, tracking, and identification, as well as both kinetic and non-kinetic effectors that can defeat airborne threats. The USAF must then train Airmen to accomplish the complete sUAV kill chain and weave threat awareness and threat response into Airmen's routines across the air base.
2. The USAF must evolve the "old" concept of counterair doctrine, employing offensive action as a defensive strategy to more effectively defend the air base from air threats posed by sUAV. Specifically, the USAF must identify target sets supporting the production and manufacture of threat sUAV and develop an intimate understanding of the networks being used to control sUAV. Importantly, U.S. forces must have the authorities to affect these critical nodes.
3. The USAF must treat the air base as a weapon system to achieve the right balance of force generation and force protection, shifting the focus of the BDOC from defending against ground threats to defending against air threats and fighting through attack. Training

Airmen to plan to defend an air base and to operate the defensive systems required while under threat expands on existing battlefield management skill training.

4. The U.S. Air Force should also develop DPPs to directly tie air base defense to the generation of aircraft and the protection of base assets. A low threat might call for very few defensive measures as Airmen continue to focus on accomplishing their primary jobs, while higher DPPs might direct the immediate launching of aircraft, "flushing the base" to avoid inbound threats. Threat mitigation measures could extend into the electromagnetic spectrum, with Airmen jamming certain bandwidths to deny access to inbound threats. These postures must be regularly exercised to ensure seamless C2 and an innate understanding of the postures by Airmen.
5. The USAF must acquire cost-effective airborne early warning and defeat capabilities for sUAV, ensuring defense-in-depth for air bases while providing a layer of protection for fielded forces. Air base threat awareness provided by point defense radars alone is insufficient for base defense. Large numbers of sUAV will quickly overwhelm the air base effectors. Airborne early warning is required to provide sufficient reaction time, as personnel require sufficient time to transition from the mission of launching aircraft to defending the base. Fielding aircraft with the range and loiter time to deliver this capability cost-effectively, like the MQ-9, can buy crucial defense-in-depth for awareness and prosecution that air bases do not currently have.
6. The USAF must evolve and operationalize policies that deliberately manage the use of the EM spectrum at air bases and across the battlespace. These lessons must inform wider EMSO implementation considerations under the Joint Force Commander.

Failure to act places unacceptable levels of risk on every air base. The news is replete with examples of inadequate defense—from Russian attacks on Ukraine to hits U.S. bases took during Operation Epic Fury. Moreover, reducing these vulnerabilities is essential to the U.S. Air Force's ability to reliably provide the airpower that is in constant demand, the indispensable element of joint force operations around the globe. Without resilient air bases, there is no reliable sortie generation; without sortie generation, there is no sustained airpower. ✪

Endnotes

1. Stacie Pettyjohn and Molly Campbell, *Countering the Swarm: Protecting the Joint Force in the Drone Age* (Washington, DC: Center for a New American Security [CNAS], September 2025), p. 20.
2. Martin Fornusek, "Russia Can Produce up to 2,700 Shahed-type Drones Per Month, Intelligence Says," *The Kyiv Independent*, September 6, 2025.
3. "Russian Offensive Campaign Assessment, October 3, 2025," Institute for the Study of War, October 3, 2025.
4. Hanna Arhirova, "Ukraine Says it Shot Down 33,000 Russian Drones in March, a Monthly Record," *Associated Press*, April 28, 2026,
5. Fornusek, "Russia Can Produce up to 2,700 Shahed-type Drones Per Month."
6. Kateryna Zakharchenko, "'We're Building Our Own Arsenal': Zelensky Says Ukraine Making 'Very Good' Progress on Missile, Drone Production," *Kyiv Post*, November 3, 2025.
7. "Operation Epic Fury: Fact Sheet," U.S. Central Command, April 6, 2026.
8. Paul J. Springer, "Iran's Military Forces Combine State-of-the-Art Drones and Hackers with Out-of-Date Conventional Weapons," *The Conversation*, April 15, 2026.
9. Chris Gordon and Stephen Losey, "Key E-3 AWACS Damaged in Iranian Attack on Saudi Air Base," *Air & Space Forces Magazine*, March 28, 2026; and Ron Bousso, "Big Oil offers reality check to Trump's Venezuela dream," *Reuters*, January 12, 2026.
10. Ibrahim Naber, "Inside Iran's Weapons Arsenal," *Business Insider*, April 15, 2026; Springer, "Iran's Military Forces"; and Bousso, "Big Oil offers reality check."
11. Linda Bilmes, "Why is the War in Iran so Expensive?" Harvard Kennedy School, April 7, 2026.
12. Jack Watling, "How Cheap Drones are Transforming Warfare in Ukraine," *The Economist*, February 5, 2024.
13. Neil Hollenbeck et al., "Calculating the Cost-Effectiveness of Russia's Drone Strikes," *Commentary*, CSIS, February 19, 2025; and Bilmes, "Why is the War in Iran so Expensive?" The Harvard Kennedy School analysis puts Iranian-produced Shahed drones at a cost of about $30,000 each.
14. Hollenbeck et al., "Calculating the Cost-Effectiveness of Russia's Drone Strikes."
15. Joint Pub 3-30 defines UAS by Group numbers. Joint Publication 3-30, Joint Air Operations, April 28, 2025. Available via FAA website.
16. Based on an interview with Ukrainian F-16 pilot detailing challenges of intercepting Russian Shahed drones over Ukraine on October 6, 2025.
17. Ashley Roque, "For Europe's 'Drone Wall,' Detecting Threats is Challenge Number One: Officials," *Breaking Defense*, November 24, 2025.
18. Roque, "For Europe's 'Drone Wall.'"
19. Elisabeth Gosselin-Malo, "Of Fiber-Optics and FPVs – 6 Questions with a Ukrainian Drone Trainer," *Defense News*, November 7, 2025.
20. Gosselin-Malo, "Of Fiber-Optics and FPVs – 6 Questions with a Ukrainian Drone Trainer."
21. Howard Altman and Tyler Rogoway, "Russian Fiber-Optic Drones and Now Reaching Into Ukrainian Cities Deep Behind the Lines," *The War Zone*, October 6, 2025.
22. David Hambling, "Russia Has an Arsenal of New AI Drones Built with Smuggled Nvidia Chips," *Forbes*, August 8, 2025.
23. "Department of Defense Strategy for Countering Unmanned Systems," Fact Sheet, Department of Defense, December 5, 2024.
24. Kateryna Bondar, "How Ukraine's Operation 'Spider's Web' Redefines Asymmetric Warfare," *Critical Questions*, CSIS, June 2, 2025.
25. Benjamin Jensen, "Ungentlemanly Robots: Israel's Operation Rising Lion and the New Way of War," *Commentary*, CSIS, June 13, 2025.
26. Alan Vick et al., *Air Base Defense: Rethinking Army and Air Force Roles and Functions* (Santa Monica, CA: RAND Corporation, 2020), p. 95.
27. Based on personal interviews with members of Air Forces Central Headquarters AFCENT/A38 TAC Command and Control and Counter UAS.
28. Matthew Cox, "Air Force Creating New Job Specialty in Base Air Defense," *Air & Space Forces Magazine*, June 30, 2026.
29. Jake Epstein, "Ukraine proved this drone-killer works. Now, the West is giving it a shot," *Business Insider*, November 18, 2025.
30. Department of Defense Directive (DODD) 3000.09, "Autonomy in Weapon Systems," January 2023.
31. Kelley M. Sayler, *Defense Primer: U.S. Policy on Lethal Autonomous Weapon Systems* (Washington, DC: Congressional Research Service [CRS], January 2, 2025).
32. Tyler Rogoway, "Everything You Ever Wanted to Know About the Navy's Ever-Evolving Aegis Combat System," *The War Zone*, March 4, 2021.
33. Thomas Newdick and Tyler Rogoway, "MQ-9B Airborne Early Warning Variant Could Fill Major Aerial Surveillance Gaps," *The War Zone*, June 17, 2025.
34. David Hambling, "Ukraine Switches Tactics to Defeat Altitude Shahed Drone Attacks," *Forbes*, September 12, 2024.
35. Arun Bishnoi, "U.S. Awards BAE Systems $1.7 Billion APKWS Contract," *Overt Defense*, December 22, 2025.
36. Stephen Losey, "Drone-Killing Drone: Air Force Test APKWS Laser-Guided Rockets on MQ-9," *Air & Space Forces Magazine*, May 12, 2026.
37. Rudy Ruitenberg, "Ukraine Claims Near-90% Air Defense Success in March as Attacks Increase," *Defense News*, April 1, 2026.
38. Katie Livingstone, "These are Ukraine's $1,000 Interceptor Drones the Pentagon Wants to Buy," *Military Times*, March 11, 2026.
39. "JIATF 401 Leads Groundbreaking US-UK Agreement on Counter-Drone Technology Standards," *ASD News*, March 26, 2026.
40. "SUADS, Small-Unmanned Air Defense System," Trust Automation, Inc. , accessed May 5, 2026.

41 Jake Epstein and Sinéad Baker, "Russia is Stepping up its Hunt for Top Targets: The Pilots Powering Ukraine's Drone Fight," *Business Insider*, October 2, 2025.
42 Oleksandr Miasyshchev, "Inside Ukraine's Hunt for Russian Drone Operators," *Arsenal*, September 20, 2025.
43 As quoted in Brandi Vincent, "Pentagon Brass Tout Destruction of Iran's Drone Arsenal, But Questions Linger About What's Left," *Defense Scoop*, April 8, 2026.
44 Warren Murray, "Ukraine war briefing: Russian drone factory attacked, 1,000km away in Tatarstan," *The Guardian*, June 15, 2025.
45 David Hambling, "Russia Shuts Down Phone Networks At Night To Stop Drone Attacks," *Forbes*, December 5, 2025.
46 Max Hunder, "Ukraine working with SpaceX to stop Russia from using Starlink to guide drones," *Reuters*, January 29, 2026.
47 Hunder, "Ukraine working with SpaceX."
48 Anthony Rodriguez, "MOPP-level awareness important for UCI success," *U.S. Air Force News*, June 28, 2007.
49 Fifth generation (5G) networks interfere with many military applications including radio communications and air defense radars. Other 5G proposals threaten to interfere with GPS signals. Stéphane Ricciardi and Cédric Souque, "Modern Electromagnetic Spectrum Battlefield: From EMS Global Supremacy to Local Superiority," *Prism* 9, no. 3, NDU Press, November 18, 2021.
50 Ricciardi and Souque, "Modern Electromagnetic Spectrum Battlefield."
51 Sinéad Baker, "Ukraine's Electronic Warfare Fight Against Russian Drones is so Chaotic That Its Own are Getting Caught in the Crossfire," *Business Insider*, August 19, 2025.
52 CJCSM 3320.01D, "Chairman of the Joint Chiefs of Staff Manual, Joint Electromagnetic Spectrum Operations," January 24, 2025.
53 Joint Publication 3-30, available via FAA website.
54 *A Comprehensive Approach to Countering UAS* (Kalkar, DE: NATO Joint Air Power Competence Centre, 2021); and Dan Gettinger et al., "The Drone Database," CNAS.
55 Larisa Brown, "We Reinvent Anti-Drone Weapons Every Month. If We Don't We Die," *The Times*, October 19, 2024.
56 Patrick Tucker, "Pentagon Pushes US Dronemakers to Innovate as Quickly as Ukraine Does," *Defense One*, June 2, 2025.
57 Tim Martin, "NATO must innovate like Ukraine or risk losing a fight with Russia: Swedish official," *Breaking Defense*, November 4, 2025.
58 Tim Lister and Kostya Gak, "Russia's Drone Revolution Heaps Pressure on Ukrainian Defenses," *CNN*, updated November 23, 2025.
59 Alex Horton, "Army Cites Glaring Failures in Drone Attack in Jordan that Killed US Troops," *The Washington Post*, April 6, 2025.
60 Horton, "Army Cites Glaring Failures in Drone Attack."
61 Mark Pomerleau, "Army awards Anduril counter-drone task order as first in new $20B 'contract vehicle'," *Breaking Defense*, March 16, 2026.
62 Eric Plummer, "AFRL awards contract for drone killer, Mjölnir; brings new drone 'hammer' to the fight," AFRL, February 25, 2022.
63 Thomas Newdick, "Drone Attack on Parked U.S. Army Black Hawk in Iraq a Harbinger of What's to Come," *The War Zone*, March 25, 2026.
64 Joseph Trevithick and Tyler Rogoway, "Iranian Attacks on Prized Missile Defense Radars are a Wake-Up Call," *The War Zone*, March 7, 2026.
65 Pettyjohn and Campbell, *Countering the Swarm*, p. 25.
66 Jake Epstein, "The US Navy's Overreliance on Top Missile Interceptors is Unsustainable in More Intense Fights, Top Admiral Warns," *Business Insider*, July 15, 2025.
67 Department of Defense, "Electromagnetic Spectrum Superiority Strategy," October 2020.
68 Pettyjohn and Campbell, *Countering the Swarm*.
69 Hope Hodge Seck, "Space Force likely to double in personnel within a decade, vice chief says," *Aerospace America*, January 22, 2026.
70 "Missile Interceptors by Cost," Missile Defense Advocacy Alliance, 2026.

About The Mitchell Institute

The Mitchell Institute educates broad audiences about aerospace power's contribution to America's global interests, informs policy and budget deliberations, and cultivates the next generation of thought leaders to exploit the advantages of operating in air, space, and cyberspace.

About the Series

The Mitchell Institute Policy Papers present new thinking and policy proposals to respond to the emerging security and aerospace power challenges of the 21st century. These papers are written for lawmakers and their staffs, policy professionals, business and industry, academics, journalists, and the informed public. The series aims to provide in-depth policy insights and perspectives based on the experiences of the authors, along with studious supporting research.

For media inquiries, email our publications team at
publications.mitchellaerospacepower@afa.org

Copies of Policy Papers can be downloaded under the publications tab on the Mitchell Institute website at
https://www.mitchellaerospacepower.org

About the Author

Brig Gen Houston Coantwell, USAF (Ret.), is a Senior Resident Fellow for Airpower Studies at the Mitchell Institute for Aerospace Studies. He is an experienced airman and recognized national security expert. During his 30-year Air Force career, he served as a combat pilot, commander, and strategist, flying the F-16, MQ-9, and RQ-4 aircraft. He also served over 12 years within the Pacific and European theaters and is intimately familiar with major U.S. allies and partners, including North Atlantic Treaty Alliance (NATO) relationships. Brig Gen Cantwell also served as the Vice Superintendent of the U.S. Air Force Academy and the Commander of the U.S. Air Force Holm Center, providing a rare opportunity to shape the entire Air and Space Force officer accessions enterprise. Most recently, he stood up the Air Force's very first Warrant Officer Training School.