From Passive Victim to Active Contender

Infantry Versus Air Dominance in Modern Warfare

A Comprehensive Analytical Report

Historical Incidents, Systemic Mistakes, and the New Infantry Doctrine for Surviving and Contesting US-Style Air Operations

April 2026

Table of Contents

Executive Summary

The recurring annihilation of infantry formations by air power stands as one of the defining phenomena of post-Cold War conflict. From the pulverizing of Iraqi columns on the Highway of Death in 1991 to the systematic hunting of individual soldiers by first-person-view (FPV) drones in Ukraine from 2022 onward, a consistent pattern has emerged: infantry forces that mass, remain static, emit electromagnetic signals, and operate without integrated air defense or electronic warfare support are destroyed with devastating efficiency. The adversary responsible for establishing this paradigm is most often characterized by the "U.S. style" of warfare, an integrated system that combines persistent overhead intelligence, surveillance, and reconnaissance (ISR), a seamless sensor-to-shooter kill chain (F2T2EA), networked command and control, and precision-guided munitions delivered from platforms operating beyond the reach of ground-based defenses.

This report provides a comprehensive, evidence-based analysis of six major conflict case studies where infantry suffered catastrophic losses to air power: the 1991 Gulf War, the 1999 Kosovo campaign, the Afghanistan drone war (2001-2021), the 2003 invasion of Iraq, the 2020 Nagorno-Karabakh War, and the ongoing war in Ukraine. For each conflict, the specific mistakes are identified, categorized, and traced to systemic vulnerabilities in doctrine, technology integration, and operational discipline. The report then examines in detail the architecture of the U.S. air dominance system, dissecting the F2T2EA kill chain and the ISR platforms that make it possible, including systems such as the MQ-9 Reaper, GORGON STARE, and the Joint Direct Attack Munition (JDAM) family.

The core of the report focuses on how infantry forces can transform from passive targets into active contenders. Drawing on lessons from all six conflicts and current military research, the report presents a layered counter-framework organized around four pillars: (1) Proactive Command and Control that clears the electromagnetic and sensor environment before committing infantry to an area, (2) a new doctrine of dispersed, stealthy, and deceptive operations that makes infantry exceptionally difficult to detect and engage, (3) integrated area defense combining kinetic and non-kinetic countermeasures in a cost-effective layered architecture, and (4) counter-ISR and disruption operations designed to break the sensor-to-shooter loop. The report concludes with an assessment of training and doctrinal modernization requirements necessary to prepare infantry for the realities of drone-saturated, electronically contested battlefields. The central thesis is that air dominance is not inviolable; it can be degraded, disrupted, and contested, but doing so requires a fundamental reorientation of how infantry organizes, moves, communicates, and fights.

1. Historical Record: Infantry Annihilation by Air Power

The history of modern warfare is punctuated by episodes in which ground forces, particularly infantry, were subjected to devastating aerial bombardment that resulted in disproportionate casualties, rapid collapse of morale, and operational failure. These episodes are not isolated anomalies but rather form a consistent pattern that reveals the systemic vulnerabilities of ground forces operating under conditions of enemy air superiority or dominance. By examining six major conflicts spanning from 1991 to the present day, a clear picture emerges of the evolving threat and the persistent failure of infantry doctrine to adapt at the same pace as air power technology. Each conflict adds a new dimension to the threat matrix: from high-altitude strategic bombing in the Gulf War to the intimate, loitering drone strikes of Ukraine, the trajectory is one of increasing sensor persistence, shortened kill chains, and expanded engagement envelopes.

1.1 The Gulf War (1990-1991): The Birth of Modern Air Dominance

The 1991 Gulf War represents the most dramatic demonstration of air power annihilating ground forces in modern military history. Operation Desert Storm, launched on January 17, 1991, opened with a 39-day air campaign that systematically dismantled the Iraqi military, a force of approximately 545,000 troops stationed in Kuwait and southern Iraq, before any significant ground offensive was launched. The Iraqi army was the fourth largest in the world at the time, battle-hardened from eight years of war with Iran, and equipped with Soviet-supplied air defense systems, tanks, and artillery. Despite this formidable order of battle, the Iraqi forces proved utterly incapable of contesting the air or protecting their ground formations from aerial attack.

The most iconic incident of the war, and the one that most starkly illustrated the vulnerability of concentrated ground forces to air power, was the attack on the retreating Iraqi columns along the Kuwait City-to-Basra highway on February 26-27, 1991, an event that became known as the "Highway of Death." As Iraqi forces withdrew from Kuwait following the initiation of the coalition ground offensive, they concentrated into massive traffic jams along Highway 80, creating dense columns of military vehicles, tanks, personnel carriers, and civilian cars fleeing alongside them. Coalition aircraft, including A-10 Thunderbolt II ground-attack aircraft, F-15E Strike Eagles, F/A-18 Hornets, and AC-130 gunships, attacked these columns with devastating effect. The resulting destruction was catastrophic: estimates of Iraqi military fatalities range from 2,000 to 10,000 along a single stretch of highway, with thousands of vehicles destroyed or abandoned. The attack was not a prolonged engagement but rather a sustained, one-sided slaughter that continued for hours as aircraft circled overhead, picking off targets at will.

The systemic mistakes that led to this catastrophe were multiple and fundamental. First, the Iraqi forces concentrated into massive, predictable formations along a limited number of roads, creating high-value targets that were impossible to miss. Their withdrawal route was entirely predictable, constrained by the terrain and available road infrastructure. Second, the Iraqi air defense network, which had been heavily degraded during the preceding 39 days of air operations, provided no meaningful protection. Surface-to-air missile (SAM) sites had been destroyed, radar systems jammed or eliminated, and communication networks severed, leaving the columns entirely exposed. Third, the Iraqi forces lacked any meaningful electronic warfare capability to disrupt coalition targeting. They could not jam coalition aircraft communications, spoof radar systems, or deploy decoys. Finally, Iraqi command and control was paralyzed; units on the ground received no effective warning or coordinated defensive instructions. The Gulf War established the template for how a technologically superior air campaign can systematically destroy a numerically superior ground force.

1.2 Kosovo (1999): Air Power Alone and the Limits of Ground Defense

Operation Allied Force, the NATO air campaign against the Federal Republic of Yugoslavia from March 24 to June 10, 1999, demonstrated that air power could achieve strategic objectives without a corresponding ground invasion, while simultaneously revealing the extreme difficulty ground forces face when operating under persistent aerial surveillance and strike. Over 78 days, NATO flew approximately 38,000 combat sorties, striking targets across Serbia and Kosovo with precision-guided munitions. While the primary targets were fixed infrastructure such as bridges, command bunkers, industrial facilities, and air defense sites, Yugoslav ground forces operating in Kosovo were also subjected to sustained aerial interdiction. NATO air operations killed an estimated 276 Serbian military and police personnel during the campaign, though the actual figure is likely higher given the difficulty of verifying casualties in a contested environment.

The Yugoslav army (VJ) demonstrated a notable degree of tactical competence in adapting to air dominance, employing extensive camouflage, concealment, and deception (CCD) measures. They dispersed their forces into small units, constructed extensive decoy positions including fake tanks, artillery pieces, and SAM sites made from wood and canvas, and maintained strict emission control to reduce their electronic signature. These tactics were partially successful; NATO struggled for weeks to locate and engage Yugoslav ground forces in the field, and post-conflict analysis revealed that a significant proportion of NATO strikes had hit decoys rather than real targets. However, the Yugoslav forces were ultimately unable to maneuver freely or conduct offensive operations. Their CCD measures allowed them to survive, but not to contest NATO's control of the battlespace. The campaign demonstrated that passive defense, while necessary, is insufficient; without the ability to strike back at the sensor or shooter, ground forces can only endure, not prevail.

1.3 Afghanistan (2001-2021): The Drone War and Persistent ISR

The Afghanistan conflict introduced a paradigm shift in air-ground engagement through the institutionalization of armed unmanned aerial vehicles (UAVs) as persistent overhead hunters. Unlike the Gulf War, where air strikes were predominantly delivered by manned aircraft operating in strike packages, the Afghanistan theater saw the MQ-1 Predator and its successor, the MQ-9 Reaper, evolve from surveillance platforms into armed hunter-killers that could loiter over a target area for up to 27 hours, tracking individuals and small groups with high-resolution cameras and synthetic aperture radar (SAR) before striking with Hellfire missiles or precision-guided bombs. The MQ-9 Reaper, equipped with GORGON STARE wide-area surveillance sensors and the VADER (Vehicle and Dismount Exploitation Radar) system, could monitor an area of up to 100 square kilometers simultaneously, automatically detecting and tracking dismounted personnel and vehicles. This represented a fundamental change in the sensor-to-shooter timeline: where a fighter jet might have a "loiter time" measured in minutes over a target area, a Reaper could maintain unblinking surveillance for a full day, waiting for the optimal moment to strike.

The impact on insurgent and Taliban infantry was profound. The drone campaign in Pakistan and Afghanistan resulted in the deaths of an estimated 81 high-level insurgent leaders and thousands of low-level fighters between 2004 and 2018. The constant overhead presence created a pervasive psychological effect: insurgents could never be certain whether they were being observed at any given moment, leading to severe operational paralysis. Meetings, gatherings, and movements became hazardous activities that invited precision strikes. The Taliban adapted over time by enforcing strict communications discipline, reducing the size of their operational cells, avoiding predictable patterns, and using terrain and weather to their advantage. However, these adaptations were reactive and came at the cost of operational tempo and effectiveness. The Afghanistan experience demonstrated that persistent ISR combined with precision strike creates an environment where even highly dispersed, clandestine infantry forces face existential risk, and where the primary survival strategy is to minimize signature rather than confront the threat directly.

1.4 Iraq 2003: Operation Iraqi Freedom and Networked Warfare

The 2003 invasion of Iraq represented an evolution of the air dominance paradigm demonstrated in 1991, now enhanced by advances in networked warfare, precision targeting, and real-time intelligence sharing. The "shock and awe" campaign that opened the invasion combined massive strikes on command and control targets with a concurrent ground offensive that moved faster than any military operation in history. The Iraqi army, numbering approximately 375,000 regular troops and additional Republican Guard and Special Republican Guard formations, was systematically dismantled over a period of approximately three weeks. While much of the Iraqi army simply dissolved as units abandoned their positions, those that did stand and fight were rapidly overwhelmed by the combination of precision air strikes and advancing ground forces. The Battle of Nasiriyah and the initial resistance at the Karbala Gap demonstrated that even when Iraqi infantry attempted to mount a conventional defense, coalition air power was able to identify and engage defensive positions with such speed and precision that coherent resistance collapsed within hours.

The key mistake of Iraqi forces in 2003, beyond the inherited vulnerabilities of mass concentration and absent air defense, was the failure to appreciate the speed of the networked kill chain. In 1991, the Iraqis had weeks of bombardment before ground forces advanced. In 2003, the air campaign and ground offensive were simultaneous, with targeting data flowing from airborne sensors to ground commanders and back to strike aircraft in near-real-time. The Iraqi command and control system, still configured for a centralized, hierarchical decision-making model, could not react fast enough. Defensive positions were identified, targeted, and destroyed before reinforcements could be dispatched or counter-orders issued. This foreshadowed the challenge that all future infantry forces would face: the sensor-to-shooter timeline had compressed to minutes, and only forces organized for extreme decentralization and rapid decision-making at the lowest level could hope to survive.

1.5 Nagorno-Karabakh (2020): The Drone Revolution

The Second Nagorno-Karabakh War of 2020 marked a watershed moment in the history of air-ground warfare and is widely regarded as the first conflict in which unmanned systems played the decisive role in determining the outcome. Azerbaijan, equipped with Turkish-made Bayraktar TB2 medium-altitude long-endurance (MALE) drones and Israeli-made Harop loitering munitions, systematically destroyed Armenian air defense systems, armored vehicles, artillery positions, and infantry concentrations over a 44-day conflict. The Bayraktar TB2, carrying laser-guided munitions with a strike radius of up to 8 kilometers, provided Azerbaijan with persistent ISR and precision strike capability at a fraction of the cost of manned aircraft. The Harop, a "kamikaze" loitering munition that could circle above a target area for hours before diving onto a target, proved devastating against static positions and concentrations of personnel.

Armenian forces suffered catastrophic losses, including the destruction of hundreds of armored vehicles, multiple SAM systems (including the advanced S-300 and Tor-M2), and an unknown but significant number of infantry casualties.

The Nagorno-Karabakh War exposed a new dimension of vulnerability for infantry: the democratization of precision air power. Previously, the kind of persistent ISR and precision strike that characterized U.S. operations was available only to the most technologically advanced militaries. The TB2 and Harop demonstrated that relatively inexpensive, commercially derived systems could achieve similar effects against a conventionally equipped opponent. Armenian infantry, trained and equipped for a more traditional combined-arms conflict, found themselves without effective countermeasures. Their air defense systems were the first targets destroyed, after which Armenian ground forces were exposed to relentless drone surveillance and strike. The lesson was unambiguous: in any future conflict, even against a non-superpower opponent, infantry must be prepared to operate under persistent drone surveillance and must possess organic counter-drone capabilities.

1.6 Ukraine (2022-Present): The FPV and Loitering Munition Era

The ongoing war in Ukraine has brought the threat to infantry to its most extreme and intimate form. Beginning in spring 2022, the proliferation of commercial off-the-shelf (COTS) drones, particularly the Chinese-made DJI Mavic series, revolutionized battlefield awareness by enabling both sides to detect enemy positions and movements beyond visual range with unprecedented resolution and frequency. However, the truly transformative development has been the mass deployment of first-person-view (FPV) drones carrying explosive payloads. These inexpensive systems, often built from commercially available components at a cost of $500 to $2,000 per unit, are manually piloted by operators using real-time video feeds and directed to crash into individual soldiers, vehicles, and fortifications with precision that rivals laser-guided munitions. The result has been a form of warfare in which individual infantrymen can be hunted and killed by overhead drones with the same lethality previously reserved for aircraft-delivered bombs, but at a fraction of the cost and with far greater persistence.

The impact on infantry tactics has been revolutionary. FPV drones have resulted in elongated front lines characterized by trench warfare, extremely low troop concentration, and slow advances. Any concentration of forces, whether for an assault, a resupply convoy, or a command meeting, invites immediate drone detection and subsequent strike by loitering FPVs or artillery guided by drone observation. The casualty rates among infantry have been severe, with FPV drone strikes producing an estimated 22% head and neck injury rate among affected personnel, consistent with the pattern of air-dropped munitions. Both sides have adapted extensively, developing electronic warfare systems to jam drone control signals, deploying anti-drone nets and screens over defensive positions, and dispersing infantry into increasingly small units. Ukraine has successfully intercepted over 80% of Russian Shahed-136 loitering munitions using a mix of anti-aircraft missiles, small arms, and electronic jamming, demonstrating the viability of layered, low-cost defenses. However, the fundamental challenge remains: infantry on the modern battlefield can be seen from above at all times and struck with precision at minimal cost. The Ukraine experience represents the current apex of the air threat to ground infantry and serves as the primary laboratory for counter-tactics development.

Conflict	Primary Air Threat	Key Infantry Mistake	Lesson Learned
Gulf War 1991	Manned strike aircraft, strategic bombing	Mass concentration on highways, absent air defense	Mass is lethal under air supremacy
Kosovo 1999	NATO PGMs, persistent patrol	Insufficient CCD, inability to maneuver offensively	Passive defense allows survival but not victory
Afghanistan 2001-21	Armed UAVs (MQ-1/MQ-9), persistent ISR	Predictable patterns, inadequate EM discipline	Persistent ISR eliminates temporal sanctuary
Iraq 2003	Networked strike packages, real-time targeting	Centralized C2 too slow for compressed kill chain	Kill chain speed demands decentralized response
Nagorno-Karabakh 2020	MALE drones (TB2), loitering munitions (Harop)	No layered air defense, conventional posture	Drone precision is democratized and affordable
Ukraine 2022-present	FPV drones, COTS UAVs, Shahed-136	Trench exposure, FPV vulnerability, inadequate C-UAS	Individual soldier is now a precision target

Table 1. Summary of Air Power Threats and Infantry Mistakes Across Major Conflicts

2. Understanding the Adversary: The U.S. Air Dominance System

To effectively counter a threat, one must first understand its architecture and operational logic. The "U.S. style" of air-ground warfare is not simply a matter of having better aircraft or more bombs; it is an integrated system that links sensors, decision-makers, and shooters into a seamless, networked kill chain. Understanding this system, specifically the F2T2EA kill chain and the ISR platforms that feed it, is essential for identifying the points at which infantry forces can interpose disruption and degradation.

2.1 The F2T2EA Kill Chain: Find, Fix, Track, Target, Engage, Assess

The kill chain is the foundational concept of modern precision warfare, formalized by the U.S. Air Force in the 1990s as F2T2EA (Find, Fix, Track, Target, Engage, Assess). Each step represents a discrete phase in the process of locating, identifying, and destroying a target, and the speed at which the entire chain can be executed determines the lethality of the system. In the 1991 Gulf War, the kill chain from detection to engagement for time-sensitive targets could take hours. By 2003 in Iraq, it had been compressed to tens of minutes. Today, with persistent ISR platforms providing real-time streaming video and automated target recognition, the kill chain for a pre-planned target can be executed in minutes, and for a target of opportunity, the timeline from detection to strike can be as short as single-digit minutes.

The "Find" phase involves the initial detection of a potential target by any sensor in the network, including satellites, high-altitude UAVs like the RQ-4 Global Hawk, tactical UAVs like the MQ-9 Reaper, manned reconnaissance aircraft, SIGINT collection platforms, and ground-based sensors. The "Fix" phase involves precisely determining the location of the detected entity, typically through geolocation of electronic emissions, SAR imaging, or multi-source intelligence fusion. The "Track" phase maintains continuous surveillance of the target to build a pattern-of-life profile and confirm its identity as hostile. The "Target" phase involves selecting the appropriate weapon system and delivery platform based on the target type, location, collateral damage constraints, and availability. The "Engage" phase is the actual delivery of the munition, which may be a Hellfire missile from a Reaper, a JDAM from a fighter jet, or a loitering munition. Finally, the "Assess" phase uses post-strike imagery to determine whether the target was successfully engaged and to identify any follow-on targets. Each phase represents a potential point of disruption for counter-tactics: if infantry can prevent detection (break Find), prevent precise location (break Fix), evade tracking (break Track), spoof targeting (break Target), or defeat the engagement itself (break Engage), the kill chain is broken and the infantry survives.

2.2 Persistent ISR Architecture

The backbone of U.S. air dominance is its Intelligence, Surveillance, and Reconnaissance architecture, a layered system of sensors operating from space, the air, and the ground that provides near-continuous coverage of the battlespace. At the highest altitude, satellite constellations provide periodic but wide-area surveillance, capable of imaging entire regions and detecting large-scale troop movements. At medium altitude, the RQ-4 Global Hawk provides persistent surveillance at altitudes above 60,000 feet, equipped with SAR and electro-optical/infrared (EO/IR) sensors that can monitor large areas for extended periods. At tactical altitude, the MQ-9 Reaper operates at altitudes up to 50,000 feet with an endurance exceeding 27 hours, carrying the GORGON STARE wide-area surveillance system that can monitor up to 100 square kilometers simultaneously, and the VADER system specifically designed to detect and track dismounted personnel. The integration of these systems through networks like the Distributed Common Ground System (DCGS) allows video and data from any platform to be shared in near-real-time with commanders, intelligence analysts, and weapon operators across the theater. This creates a situation where a single infantryman moving in the open can be detected by a satellite pass, handed off to a Reaper for continuous tracking, identified through pattern-of-life analysis, and engaged within minutes by a Hellfire missile, all without any human on the ground ever seeing the enemy.

2.3 Precision-Guided Munitions and Loitering Systems

The strike component of the U.S. air dominance system has evolved from large-scale carpet bombing to surgical precision engagement. The Joint Direct Attack Munition (JDAM) kit, which converts unguided bombs into GPS-guided precision weapons, provides all-weather, day-or-night strike capability with a circular error probable (CEP) of approximately 5 meters. The AGM-114 Hellfire missile, the primary armament of armed UAVs, provides precision engagement of point targets, including individual vehicles and small groups of personnel, with a warhead that can be configured for blast-fragmentation or top-attack against armored vehicles. The Small Diameter Bomb (SDB) extends the engagement envelope by providing a smaller, lighter precision weapon that can be carried in larger numbers per aircraft, allowing a single sortie to engage multiple targets. Perhaps most relevant to the infantry threat is the proliferation of loitering munitions such as the Switchblade series, which combine ISR and strike capability in a single, man-portable package that can be launched, loiter over an area for up to 40 minutes, identify a target, and dive onto it with a shaped-charge warhead. These systems effectively give forward observers and small units the ability to call in precision strikes on individual infantrymen, blurring the line between artillery, air support, and direct fire.

3. Anatomy of Disaster: Systemic Mistakes That Enable Air Annihilation

The catastrophic attrition of infantry by air power is not the result of a single tactical error but rather the cumulative effect of multiple, reinforcing vulnerabilities that span tactical behavior, operational planning, and doctrinal preparation. These mistakes consistently align with the stages of the kill chain, creating predictable weaknesses that a technologically superior adversary can exploit systematically. The following analysis categorizes the six most critical systemic mistakes, drawing on evidence from every conflict examined in this report.

3.1 Over-Concentration and Predictable Movement Patterns

The single most lethal mistake infantry can make under conditions of air dominance is to concentrate forces in large, visible formations or to move along predictable routes at predictable times. This mistake appears in every conflict examined: Iraqi columns on the Highway of Death in 1991, Serbian forces massing for attempted offensives in Kosovo in 1999, Taliban gatherings targeted by drones in Afghanistan, Iraqi defensive positions in 2003, Armenian vehicles massed at crossing points in Nagorno-Karabakh, and Russian and Ukrainian reinforcements moving along known roads in Ukraine. The underlying logic is straightforward: a single precision-guided munition can destroy an area of effect measured in tens of meters, but a company of 100 soldiers concentrated in a small area presents a single, high-value target. The same munition, delivered against dispersed fire teams spread across hundreds of meters, will destroy a fraction of the force and leave the remainder combat-effective. Predictable movement patterns, including the use of the same supply routes, patrol routes, and assembly areas, create "patterns of life" that ISR systems can detect and exploit. Once a pattern is established, the adversary can position assets to ambush the force along its route at the optimal time and place, maximizing the lethality of the engagement.

3.2 Multi-Spectral Signature Management Failures

Modern sensor systems do not rely on a single modality; they operate across the visual, infrared, radar, and electromagnetic spectrums simultaneously. A unit that is well-concealed visually may be glaringly obvious in the thermal spectrum due to body heat, vehicle engine exhaust, or cooking fires. A unit that has minimized its thermal signature may still be detectable through radar due to metallic equipment, communication antennas, or movement that creates radar returns. A unit that has addressed both visual and thermal signatures may still be located through its electromagnetic emissions: radio transmissions, radar emissions from nearby systems, or even the electronic noise generated by communication equipment. The failure to implement multi-spectral CCD, meaning the simultaneous management of all detectable signatures, allows enemy sensors to seamlessly transition from detection to classification to engagement. The absence of multi-spectral CCD means that a unit is not merely suspected to be present; its presence is confirmed, its composition identified, and its location precisely determined before any weapon is launched.

3.3 Electronic Warfare and Signal Discipline Failures

In the modern electromagnetic battlespace, every radio transmission is a beacon. Units that operate with poor emission control (EMCON) protocols, using unsecured radio frequencies, maintaining continuous transmissions, and failing to employ directional antennas, broadcast their location, identity, and intentions to any adversary with a signals intelligence (SIGINT) capability. The U.S. SIGINT architecture, integrated through systems like the RC-135 Rivet Joint and various ground-based collection platforms, can triangulate radio emissions to within meters, identify the type of radio and its hierarchical level, and analyze communication patterns to determine command relationships and operational intent. This transforms the essential tool of infantry command and control, communication, into a liability that actively guides precision munitions to the unit. The failure to enforce strict EM discipline, combined with the absence of organic electronic warfare capability to jam, spoof, or otherwise degrade enemy SIGINT collection, leaves infantry units with no defense against one of the most effective targeting methods available.

3.4 Absent or Fragmented Short-Range Air Defense

The vulnerability of infantry to air power is dramatically amplified when organic short-range air defense (SHORAD) is absent, static, or poorly integrated. Modern air threats to infantry encompass a diverse portfolio: high-altitude fast jets delivering JDAMs, medium-altitude MALE drones like the TB2, low-altitude tactical UAVs providing reconnaissance and fire correction, and low-slow loitering munitions like the Shahed-136 and FPV drones. Each threat type requires a different intercept method. A single SHORAD system, whether a MANPADS or an anti-aircraft gun, cannot address all of these threats simultaneously. The absence of a layered, mobile SHORAD network that integrates sensors, kinetic effectors (missiles, guns), and non-kinetic effectors (EW jamming, directed energy) leaves critical gaps that aircraft and drones exploit. In every conflict studied, the first priority of air operations was the suppression of enemy air defenses (SEAD), and in each case, once air defenses were degraded, ground forces were exposed to unrestricted aerial attack.

3.5 Isolation from Combined-Arms Support

Infantry operating in isolation, without organic artillery support, engineer capabilities, armored protection, or dedicated ISR assets, is fundamentally unable to contest the sensor-to-shooter loop that enables air dominance. An isolated infantry unit cannot call for counter-battery fire to suppress enemy artillery that may be registering targets. It cannot rely on engineers to rapidly construct survivable positions, destroy bridges to channel enemy movements, or emplace minefields and obstacles. It lacks organic ISR to provide local situational awareness, forcing reliance on external sources that may be jammed, delayed, or unavailable. Most critically, it cannot conduct counter-strikes against identified enemy sensor platforms or launch points. Without combined-arms integration, the infantry unit is reduced to a passive target that can only absorb punishment rather than contest the battlespace. The Nagorno-Karabakh War provided the starkest illustration: Armenian infantry, once stripped of air defense and artillery support by Azerbaijani drone strikes, became helpless targets for persistent overhead surveillance and precision engagement.

3.6 Outdated Doctrine and Training for Drone-Saturated Environments

Military organizations evolve slowly, and many infantry forces continue to train for conflict models that no longer reflect battlefield reality. Training that emphasizes massed firepower, linear formations, and centralized command produces units psychologically and tactically unprepared for an environment where a single drone can identify and destroy a squad within minutes. The transition from conventional maneuver warfare to drone-saturated, electronically contested operations requires a fundamental reorientation of infantry training: soldiers must be proficient in multi-spectral CCD, EM discipline, rapid displacement drills, counter-UAS procedures, and decentralized decision-making. Units must be stress-tested against realistic scenarios involving drone swarms, persistent overhead surveillance, and degraded communications. The Ukraine war has demonstrated that soldiers who lack this training suffer disproportionate casualties, while those units that have adapted, developing tactical procedures for camouflage, dispersion, and electronic countermeasures, achieve significantly higher survival rates. The gap between legacy doctrine and current battlefield requirements represents one of the most dangerous vulnerabilities in modern infantry forces.

Mistake Category	Specific Error	Kill Chain Phase Exploited	Historical Evidence
Tactical	Over-concentration and predictable movement	Find, Fix, Track	Highway of Death (1991), FPV strikes in Ukraine
Tactical	Multi-spectral CCD failure	Find, Track, Target	IR detection of Iraqi forces (1991), VADER tracking in Afghanistan
EW/Comms	Poor EMCON and signal discipline	Find, Fix	SIGINT targeting in all conflicts
Operational	Absent/fragmented SHORAD	Engage (not disrupted)	SEAD success in Gulf, Karabakh, Iraq 2003
Operational	Isolation from combined arms	All phases (no counter)	Armenian forces in Karabakh 2020

Doctrinal	Outdated training and doctrine	All phases	All conflicts; training gap confirmed by after-action reviews

Table 2. Systemic Mistakes Mapped to Kill Chain Vulnerabilities and Historical Evidence

4. Proactive Command and Control: Area Clearance Before Deployment

The most fundamental shift required for infantry to survive under air dominance is the transition from reactive defense, attempting to survive after being detected, to proactive offense, actively degrading the adversary's ability to sense and target before committing ground forces. This concept, termed "Proactive Command and Control," holds that an area cannot be considered "cleared" simply because no enemy ground forces are visible. In a technologically advanced conflict, an area is only safe for infantry operations when its electromagnetic and sensor environment has been assessed, degraded, or controlled. This requires a systematic process of identifying enemy ISR assets, suppressing their capabilities, and creating temporary windows of reduced surveillance coverage through which infantry can maneuver.

4.1 Electromagnetic Battlespace Assessment

Before any infantry operation is conducted in a contested environment, the command element must conduct a thorough assessment of the electromagnetic battlespace. This involves mapping all known or suspected enemy sensor platforms, including high-altitude ISR aircraft operating at stand-off ranges, tactical UAVs providing local coverage, ground-based radar installations, SIGINT collection platforms, and satellite overpass schedules. The assessment should identify which frequency bands are being monitored, the approximate location and coverage area of enemy EW systems, and the likely position of relay nodes and communication hubs that support the adversary's sensor network. This electromagnetic order of battle (EOB) becomes the foundation for planning suppression operations. Without this assessment, any infantry movement is conducted blind, with no understanding of which sensors are observing the area and from what direction. The assessment must be continuously updated as enemy assets are redeployed or new platforms detected, and the results must be disseminated to all subordinate units as part of the operations order.

4.2 EW Area Denial and SIGINT Countermeasures

The primary tool for creating temporary windows of reduced surveillance is electronic warfare area denial. This involves deploying specialized jamming modules to create temporary exclusion zones for enemy drones or to deny specific frequency bands over a planned route or objective. Man-portable, rail-mounted jamming modules have been developed specifically for this purpose, designed to create an area denial effect against unmanned aerial systems by blanketing a corridor with radio frequency noise. These systems prevent enemy drones from receiving commands from their operators, deny them access to GPS signals for navigation, and can force them to crash or revert to pre-programmed loiter patterns. By creating a "bubble" of electronic noise along the planned route of advance, the command element can significantly reduce the risk of infantry being tracked and targeted by remotely piloted systems during the most vulnerable phase of the operation: movement.

SIGINT countermeasures complement EW area denial by actively degrading the adversary's ability to locate and identify friendly forces through their communications. This can involve "hunting" for enemy SIGINT collection platforms through direction-finding to pinpoint their location, or through deceptive emissions. By flooding the airwaves with false traffic or mimicking friendly transmission patterns, a unit can saturate and confuse enemy SIGINT analysts, making it difficult to distinguish real activity from deception. This electronic deception can be used to lure enemy sensors toward decoy positions or to mask the true location and movement of the actual infantry force. The successful execution of SIGINT countermeasures requires close coordination between EW specialists, intelligence analysts, and ground force commanders to ensure that suppression efforts are synchronized with the timing and location of the infantry's movement.

4.3 Kinetic Suppression of Enemy Sensor Networks

Where EW alone is insufficient, kinetic means must be employed to destroy or degrade enemy sensor platforms before infantry operations commence. If intelligence confirms the presence of a high-value radar installation, a command bunker housing ISR processing nodes, or an airfield from which ISR aircraft operate, these can be designated for preemptive strike by long-range artillery, standoff missiles, or special operations forces. The downing of a U.S. RQ-4 Global Hawk by Iran in June 2019, while disputed in terms of the exact location of the incident, underscored the vulnerability of even high-altitude, high-value ISR assets to capable integrated air defense systems. While not every infantry unit will have direct access to long-range strike assets, the principle is clear: if the source of surveillance can be destroyed or degraded before an operation begins, the risk to ground forces is dramatically lowered. This requires timely and accurate intelligence, a responsive targeting process, and the integration of long-range fires into the infantry support plan.

4.4 C2 Integration and Synchronized Multi-Domain Operations

The integration of these capabilities requires a fundamental evolution in C2 structure. Traditional command posts and staff sections must incorporate dedicated EW officers and SIGINT analysts who are treated as equal partners in the operational planning process. They are not support functions but integral components of the battle plan. Their task is to assess the electromagnetic threat environment, recommend courses of action to mitigate it, and coordinate the application of EW effects with the movement of friendly forces. The operational sequence might unfold as follows: first, a SIGINT asset locates an enemy radar site; second, an EW asset prepares to jam the associated frequency; third, a long-range missile system stands ready to destroy the site if jamming is insufficient; and fourth, the infantry unit moves through the area once the site is confirmed as degraded or offline. This coordinated, proactive approach is the essence of turning the tables on air dominance, shifting the focus from hiding from the sensor to actively defeating the sensor itself before infantry is exposed.

5. The New Infantry Doctrine: Dispersed, Stealthy, Deceptive

In response to the pervasive threat of air surveillance and precision strike, the most fundamental adaptation required in infantry tactics is the deliberate rejection of mass in favor of dispersion, decentralization, and deception. This new doctrine acknowledges that survival under conditions of air dominance is not achieved through greater firepower or stronger fortifications, but through a combination of agility, stealth, and the ability to manipulate the enemy's perception of the battlefield. The core principles involve breaking up into small, autonomous cells, mastering multi-spectrum concealment, and employing aggressive deception to confuse and mislead adversary sensors.

5.1 Dispersion and Mission Command

The cornerstone of the new infantry doctrine is the principle of dispersion and decentralization. Instead of forming platoons and companies into large, linear formations, modern infantry must operate in small, highly mobile fire teams or "cells," typically of four to six soldiers, guided by the concept of "mission command." Mission command empowers junior leaders to make decisions based on local situations without waiting for orders from a centralized command post. The primary advantage of dispersion is twofold: first, it drastically reduces the lethality of a single precision strike. While a single bomb or missile can devastate a company-sized formation concentrated in an area of a few hundred meters, its effect on several scattered fire teams dispersed across a kilometer or more is minimal. Second, it complicates the adversary's targeting problem immensely. An enemy sensor operator must now identify, classify, and prioritize multiple smaller targets across a wider area, increasing cognitive load and the probability of error. Dispersal extends beyond just personnel: logistics, command posts, ammunition resupply points, and casualty collection stations must also be decentralized and staggered to avoid creating high-value, static concentrations that invite precision strikes.

5.2 Multi-Spectral Camouflage, Concealment, and Deception (CCD)

Survival in the 21st-century battlespace depends on masking all detectable signatures simultaneously. This goes far beyond traditional visual camouflage using foliage and dirt. Multi-spectral CCD involves the use of specialized netting that can obscure visual, infrared, and radar signatures; thermal blankets designed to mask the heat generated by personnel, equipment, and engines; and radar-absorbent materials applied to vehicles and equipment to reduce radar cross-section. The Ukraine conflict has starkly illustrated the enduring importance of deception tactics: both sides have extensively used decoys, both physical and electronic, to draw fire away from real assets. Physical decoys include inflatable dummies of vehicles and artillery pieces, while electronic decoys generate false thermal or radio frequency emissions to mimic a real unit. The effectiveness of CCD measures is enhanced by a deep understanding of terrain. Using features like reverse-slope positions, where troops are hidden behind a hillcrest out of sight of overhead sensors operating at an angle, dense forest canopy that breaks both visual and infrared line-of-sight, and the complex clutter of urban environments can provide natural concealment that complements artificial CCD materials.

5.3 Aggressive Deception Operations

Deception in the new infantry doctrine goes beyond passive concealment to encompass active manipulation of the enemy's perception. One powerful technique is the maintenance of decoy networks, both static and mobile, that can be activated to simulate the activities of a larger force. A decoy network might include inflatable vehicle models positioned to resemble a motorized infantry company, with associated heat sources to generate thermal signatures, radio transmitters emitting traffic patterns consistent with a command post, and movement along fake supply routes. These decoys draw enemy ISR assets and precision munitions away from the location of the real force, wasting the adversary's resources and buying time for actual infantry operations. GPS and radio spoofing represents another critical deceptive measure. By broadcasting false GPS coordinates or manipulating radio signals, a unit can trick enemy targeting systems into calculating an incorrect location for the emitter, causing munitions to fall harmlessly elsewhere. This requires sophisticated EW equipment but offers a potent way to turn the enemy's own precision against them, using their reliance on accurate geo-location as a vulnerability.

5.4 Shoot-and-Scoot and Rapid Displacement

The "shoot-and-scoot" or "fire-and-displace" tactic is essential survival doctrine for infantry operating under air dominance. The principle is straightforward: any activity that creates a detectable signature, whether firing a weapon, establishing a radio transmission, lighting a fire, or conducting a resupply operation, must be immediately followed by a displacement to a new, previously prepared concealed position. The time window between signature generation and potential engagement can be as short as a few minutes, especially when persistent ISR platforms are overhead. Infantry units must rehearse displacement drills until they become automatic: designated alternate positions must be pre-surveyed and prepared with camouflage materials, movement routes between positions must be planned to avoid open terrain and predictable pathways, and the entire unit must be able to vacate a position within minutes. The Ukrainian experience has shown that units which maintain strict displacement discipline, never remaining in any position longer than necessary, suffer significantly fewer casualties than those that linger. This requires exceptional physical fitness, disciplined junior leadership, and a cultural shift from viewing a prepared defensive position as a "home" to viewing it as a temporary waypoint.

5.5 Terrain and Weather Exploitation

Infantry must leverage the natural advantages of terrain and weather to degrade the effectiveness of enemy sensors and precision weapons. Terrain features that break line-of-sight from above are particularly valuable: deep valleys, ravines, cave systems, and dense urban areas provide natural screening from overhead surveillance. Underground facilities, whether purpose-built bunkers or improvised cellar and basement positions, offer near-complete protection from all aerial threats except the largest penetrator munitions. Reverse-slope positions, where the unit is positioned behind the military crest of a hill so that it cannot be directly observed from above, remain one of the most effective passive defense measures available to infantry. Weather also plays a critical role: low cloud ceilings, fog, heavy rain, and snow degrade the effectiveness of optical and infrared sensors, while thick atmospheric conditions can scatter laser designator beams and degrade laser-guided weapon accuracy. Night operations, while not providing complete protection due to the widespread availability of thermal imaging and night-vision equipment, still offer advantages in terms of reduced visual detection range and increased difficulty for FPV drone operators. Operations timed to coincide with adverse weather conditions or darkness can significantly reduce vulnerability to air surveillance and precision strike.

6. Integrated Area Defense: Layered Protection Architecture

While dispersed maneuver and deception reduce a unit's vulnerability, they do not eliminate the threat posed by incoming aerial ordnance. To survive and operate effectively in a contested airspace, infantry must operate within an integrated defensive umbrella that combines kinetic and non-kinetic countermeasures in a layered architecture optimized for different threat profiles and engagement ranges.

6.1 Kinetic Countermeasures

Kinetic countermeasures remain a foundational element of air defense. These systems physically destroy or disable incoming threats. At the higher end of the capability spectrum, surface-to-air missile systems such as the Norwegian Advanced Surface to Air Missile System (NASAMS) and various MANPADS (Man-Portable Air-Defense Systems) like the FIM-92 Stinger and Igla-S are effective against fast-moving, higher-altitude threats including aircraft and cruise missiles. For slower, lower-flying threats such as tactical UAVs and loitering munitions, anti-aircraft autocannons and heavy machine guns can be highly effective when employed in a coordinated manner to create an impassable barrier of fire. The Ukrainian experience with Russian Shahed-136 loitering munitions demonstrated that even small arms, when fired in concentrated volleys, can bring down low, slow drones. The key to effective kinetic defense is layering: different systems optimized for different threat profiles, creating overlapping fields of fire so that a threat that evades one layer is engaged by the next. A forward-deployed infantry company might have a MANPADS team for high-altitude threats, autocannons for medium-altitude drones, and designated riflemen for low-altitude FPVs, all coordinated through a central air defense warning and control network.

6.2 Non-Kinetic (Soft-Kill) Countermeasures

Non-kinetic countermeasures, often termed "soft-kill" systems, represent the most rapidly evolving domain of air defense and are increasingly critical due to the unfavorable cost-exchange ratio of kinetic engagements. A standard cruise missile can cost approximately one million dollars, while a Russian Shahed-136 kamikaze drone costs approximately $20,000, and an FPV drone can cost as little as $500. Using a million-dollar missile to destroy a $500 drone is an unsustainable equation. Non-kinetic systems address this by disrupting, deceiving, or disabling aerial threats without destroying them, at a fraction of the cost per engagement.

Radio frequency (RF) jamming is the most widely deployed non-kinetic countermeasure, used to block the control link between a drone and its operator, causing the drone to lose commands, crash, or revert to a pre-programmed loiter or return-to-home mode. GNSS jamming and spoofing target the drone's navigation system, denying GPS access or feeding false coordinates. High-powered microwave (HPM) weapons emit a burst of electromagnetic energy that can fry the delicate electronics inside a drone's avionics suite, causing instantaneous failure; this technology is particularly suited for engaging drone swarms, as a single pulse can affect multiple targets. Directed energy weapons, primarily laser systems, offer precision engagement with extremely low cost-per-shot limited mainly to electricity consumption. Acoustic methods, though less developed, use intense sound waves to disrupt the gyroscopic sensors inside drones, causing loss of stability. The integration of these diverse systems into a unified command and control architecture, where detection assets like radars and optical sensors feed data to a central node that selects the most appropriate and cost-effective effector, is the direction of modern counter-UAS development.

6.3 Layered Defense Architecture and Cost-Exchange Considerations

A comprehensive area suppression plan must integrate these varied capabilities into a layered defense architecture. The U.S. 2022 Missile Defense Review explicitly recognized the need for a comprehensive approach that includes non-kinetic technologies to address the threat of low-tech, low-flying drones. In a practical deployment, a forward infantry battalion might organize its air defense as follows: at the outermost layer (5-10 km), EW systems create a wide jamming corridor that degrades enemy UAV navigation and command links; at the middle layer (2-5 km), SHORAD missile systems and autocannons engage any threats that penetrate the EW barrier; and at the innermost layer (0-2 km), directed energy weapons, HPM devices, and small-arms fire provide point defense against individual drones or loitering munitions that evade outer layers. Each layer is progressively cheaper to operate per engagement, ensuring that the defense is economically sustainable even against large numbers of inexpensive threats.

Technology Type	Example System	Mechanism	Target Profile
Kinetic: MANPADS	FIM-92 Stinger, Igla-S	IR-guided missile interception	Aircraft, helicopters, high-altitude drones
Kinetic: Autocannon	ZU-23-2, Pantsir-S1 guns	Projectile impact	Low-altitude drones, cruise missiles
Non-Kinetic: RF Jammer	Repellent-1, Krasukha-4	Blocks drone control link	Radio-controlled UAVs, FPV drones
Non-Kinetic: GNSS Spoof	Various EW modules	Feeds false GPS coordinates	GPS-guided drones, loitering munitions
Non-Kinetic: HPM	CHAMP, Epirus Leonidas	EM pulse fries electronics	Drone swarms, UAS clusters

Non-Kinetic: Laser	Raytheon HELWS	Focused energy burns airframe	Individual small drones, line-of-sight targets

Table 3. Counter-UAS Technology Portfolio for Infantry-Level Air Defense

7. Counter-ISR and Disruption Operations: Breaking the Kill Chain

The sensor-to-shooter kill chain is only as strong as its weakest link. Counter-ISR and disruption operations target the early phases of the kill chain, specifically the Find, Fix, and Track phases, with the objective of preventing the adversary from establishing the situational awareness necessary to deliver precision fires. By attacking the enemy's ability to see, locate, and track friendly forces, infantry units can deny the adversary the targeting data required to initiate engagement, effectively neutralizing the air threat without ever firing a shot at an aircraft.

7.1 Breaking the Sensor-to-Shooter Loop

The sensor-to-shooter loop can be disrupted at multiple points. The most direct method is physical destruction of sensor platforms through long-range artillery, surface-to-air missiles, or special operations forces. However, this requires the ability to detect and engage high-value, often well-protected targets. A more accessible method for infantry-level forces is EW disruption: jamming the data links that transmit sensor data from platforms to ground stations, or jamming the command links that control sensor platforms. If a drone cannot transmit its video feed to an operator, it becomes an expensive blind spot in the sky. If a satellite cannot downlink its imagery, the intelligence it has gathered is trapped on the platform. Additionally, physical obscuration, using smoke, dust, or purpose-generated aerosol clouds, can degrade optical and infrared sensor performance over specific areas, providing temporary windows for movement. The key principle is that the kill chain requires continuous data flow; any interruption in that flow, whether through destruction, jamming, or obscuration, introduces delays and uncertainty that can be exploited by ground forces.

7.2 Decoy Networks and Signature Management

Decoy networks represent one of the most cost-effective methods of counter-ISR. By maintaining a portfolio of decoy positions, thermal emitters, RF transmitters, and inflatable vehicle models that can be rapidly deployed and activated, an infantry force can saturate the enemy's sensor grid with false targets. Each false target that the adversary investigates, classifies, and potentially engages consumes time, analyst attention, and munitions that would otherwise be directed at real forces. The Ukrainian conflict has provided extensive evidence of the effectiveness of decoys: both sides have used dummy artillery pieces, fake vehicle formations, and simulated radio traffic to draw enemy fire. When the adversary's ISR assets are being consumed by tracking and engaging decoys, real infantry forces have greater freedom of maneuver.

Signature management extends beyond decoys to include the systematic reduction of all detectable signatures: using thermal blankets for personnel and equipment, radiator shielding on vehicles, emplacing camouflage nets treated with radar-absorbent materials, and minimizing all electromagnetic emissions. The goal is to reduce the friendly force's radar, thermal, visual, and electromagnetic profile to match the background environment, making it indistinguishable from the surrounding terrain to enemy sensors.

7.3 GPS and Radio Spoofing

GPS spoofing has emerged as a particularly potent counter-ISR technique with direct implications for infantry survival. Many modern precision-guided munitions, UAVs, and surveillance systems rely on GPS for navigation and targeting. By broadcasting false GPS signals that are stronger than the authentic satellite signals, a spoofing device can cause enemy systems to calculate incorrect positions, leading drones to navigate to wrong locations, munitions to miss their targets, and ISR platforms to report incorrect coordinates. During the Ukraine conflict, GPS spoofing has been used extensively by both sides, with Russian EW systems creating "GPS denial zones" that disrupt Ukrainian drone operations and Western precision munition guidance. For infantry forces facing U.S.-style precision threats, GPS spoofing offers a way to degrade the accuracy of JDAM-equipped aircraft, disrupt the navigation of loitering munitions, and interfere with the geo-location capabilities of enemy ISR platforms. The technology is becoming increasingly accessible, with commercial GPS spoofing equipment available for relatively low cost, making it a viable tool even for non-state actors and less technologically advanced militaries.

7.4 EW Saturation and Deception

Electronic warfare saturation involves flooding the electromagnetic spectrum with noise, false signals, and deceptive emissions to overwhelm the adversary's SIGINT collection and analysis capabilities. Rather than attempting to maintain radio silence entirely, which can severely limit command and control, saturation tactics accept that some electromagnetic signature will be detectable but aim to make that signature so noisy and confusing that the adversary cannot extract actionable intelligence from it. Techniques include broadcasting on multiple frequencies simultaneously, using burst transmissions at random intervals from distributed locations, generating false command traffic that mimics real operational orders, and deploying mobile emitters that simulate the signature of larger formations. The objective is to create an electromagnetic environment so cluttered that the enemy's targeting cycle is extended from minutes to hours, buying time for infantry operations. This approach recognizes that in modern warfare, complete electromagnetic invisibility is rarely achievable; the goal instead is to make the cost of analyzing friendly emissions so high that the adversary's targeting process becomes unreliable and slow.

8. Training and Doctrinal Modernization

None of the tactical, technical, or operational countermeasures described in this report can be effective without a corresponding transformation in how infantry forces are trained and organized. The gap between legacy doctrine, designed for conventional maneuver warfare against peer adversaries, and the reality of drone-saturated, electronically contested combat is one of the most dangerous vulnerabilities in modern infantry forces. Closing this gap requires fundamental changes in training methodology, organizational structure, and institutional culture.

8.1 Drone-Saturated Environment Training

Infantry training must systematically incorporate realistic drone threat scenarios at every level, from individual skill training to brigade-level exercises. Soldiers must learn to recognize the sound and visual signature of different drone types, understand the altitude and speed profiles that indicate different threat levels, and practice immediate-action drills for drone overflight including dispersal, taking cover under overhead screening, and activating electronic countermeasures. Live-fire exercises should include drone observation and targeting of friendly forces, with the drones serving as both OPFOR intelligence assets and actual strike platforms using inert munitions or laser designators linked to artillery simulators. Units should be evaluated on their ability to conduct tactical movements while under continuous drone observation, with performance metrics including time to detection, dispersion time, and the percentage of the force that reaches its objective without being "engaged" by the drone. The psychological dimension must also be addressed: soldiers must be conditioned to operate under the constant stress of potential overhead observation and strike, a fundamentally different psychological environment from traditional combat where the primary threats are from the front.

8.2 EW-Contested Operations Training

Training for electronic warfare conditions must become as fundamental as marksmanship and physical fitness. Soldiers must be proficient in operating with degraded or denied communications, using visual signals, runners, and pre-arranged protocols when radio communications are jammed. EMCON drills must be practiced until radio silence procedures become second nature: burst transmissions only, lowest possible power settings, directional antennas aimed away from known enemy SIGINT positions, and frequency changes at random intervals. Junior leaders must be trained to make tactical decisions without constant communication with higher headquarters, exercising mission command principles under realistic conditions. Units should conduct exercises in "EM-denied" environments where all electronic communications are deliberately degraded, forcing reliance on pre-planned actions, decentralized decision-making, and physical signals. This training must extend to the use of organic EW equipment, with every infantry squad or platoon having designated EW specialists trained in the operation of portable jamming devices, direction-finding equipment, and decoy activation systems.

8.3 Cross-Training and Small-Unit Autonomy

The dispersed, cell-based infantry doctrine described in Chapter 5 requires soldiers who are cross-trained in multiple roles. In a four-man fire team operating independently, there is no room for specialists who can only perform one function. Every soldier must be capable of basic EW operation, first aid, navigation, communications, and drone identification. At least one member should be trained in the operation of MANPADS or other anti-air weapons, and at least one in the use of organic counter-UAS systems. This cross-training requirement extends to leadership: in a dispersed force, the senior soldier in any isolated cell must be prepared to assume command and make tactical decisions without external guidance. Small-unit autonomy requires a cultural shift within infantry organizations, away from rigid adherence to prescribed solutions and toward initiative, adaptability, and trust in junior leaders. Research into wearable-derived metrics for squad performance suggests that physiological and behavioral data can be used to predict how well a squad executes battle drills, offering a new tool for assessing and improving these critical skills. The ultimate measure of training effectiveness is whether an infantry unit, when deployed in a drone-saturated, EW-contested environment, can accomplish its mission while maintaining acceptable casualty rates.

9. Strategic Assessment: Can Infantry Turn the Tables?

The central question of this report is whether infantry forces can move from being passive victims of air power to becoming active contenders who survive, adapt, and contest the systems that enable air dominance. The evidence gathered from six major conflicts and current military research suggests that the answer is a qualified yes. Air dominance is not inviolable. It can be degraded through attrition of sensor platforms, disruption of targeting networks, integrated ground-based defenses, terrain exploitation, and operational tempo. However, achieving this requires treating the battlefield not as a simple infantry-versus-aircraft dynamic, but as a complex contest of sensors, networks, and logistics in which infantry plays a specific but critical role.

9.1 Inherent Limitations of Air Power

Despite its overwhelming technological advantages, air power has inherent limitations that infantry can exploit. First, air power is consumable: aircraft require fuel, munitions, maintenance, and crew rest. Even UAVs require operator shifts and mechanical servicing. A sustained campaign imposes logistical strain that limits the number of sorties and the duration of persistent surveillance. Second, air power struggles with concealment: forces that are well-hidden, whether underground, under dense canopy, or in urban terrain, present targeting challenges that even advanced sensors cannot fully overcome. The Kosovo experience demonstrated that a well-concealed ground force can survive weeks of intense aerial bombardment. Third, weather remains a significant factor: cloud cover, fog, and atmospheric conditions degrade sensor performance and can ground aircraft entirely. Fourth, the cost-exchange ratio is increasingly unfavorable for air forces: cheap drones and loitering munitions force expensive interceptors and air defense systems to expend resources disproportionate to the threat, while air-delivered munitions costing hundreds of thousands of dollars can be rendered ineffective by decoys costing hundreds. Finally, air power alone cannot hold ground. It can destroy, disrupt, and degrade, but only infantry can occupy, control, and govern territory. This fundamental truth means that infantry will always have a role, and that the contest between air power and ground forces will continue as an enduring dynamic of warfare.

9.2 Lessons from Asymmetric Adaptation

The most instructive examples of infantry successfully contesting air dominance come from asymmetric conflicts where technologically inferior forces adapted to negate the advantages of air power. The Viet Cong and North Vietnamese Army adapted to massive U.S. aerial bombardment by constructing extensive tunnel networks, dispersing into small units, using the dense jungle canopy for concealment, and restricting movements to night and adverse weather. Hezbollah in southern Lebanon in 2006 survived intensive Israeli air strikes by using pre-prepared underground bunkers, maintaining strict EMCON, and dispersing forces so effectively that Israeli air power could not locate and engage them in sufficient numbers to prevent missile launches. The Houthis in Yemen have adapted to Saudi-led coalition air superiority by dispersing into small cells, using terrain, and developing their own drone and missile capabilities to strike back. These examples share common themes: dispersion, underground or concealed positions, strict emission control, decentralized operations, and the use of terrain and weather to degrade sensor effectiveness. The tactical adaptations of these forces, while context-specific, validate the broader principles outlined in this report and demonstrate that infantry survival under air dominance is achievable when the right combination of discipline, deception, and tactical innovation is applied.

9.3 The Future Battlespace

The trajectory of military technology suggests that the air threat to infantry will intensify rather than diminish. Artificial intelligence is being integrated into ISR systems to enable automated target recognition, reducing the time from detection to engagement from minutes to seconds. Drone swarm technology, already under active development by multiple nations, promises to saturate the battlefield with dozens or hundreds of coordinated UAVs operating autonomously, overwhelming traditional point defenses. Hypersonic weapons, capable of Mach 5+ speeds, compress engagement timelines to seconds, leaving minimal time for defensive reactions. Counter-stealth technologies and advanced sensors operating across new spectral bands may reduce the effectiveness of current CCD measures. In this environment, the infantry's survival will depend increasingly on its ability to operate within an integrated multi-domain system that combines EW, cyber, space, and ground-based capabilities to contest every phase of the kill chain. The infantryman of the future will not be a lone figure with a rifle hiding from the sky; he will be a node in a networked, electronically sophisticated system that uses deception, disruption, and integrated defense to deny the adversary the situational awareness necessary for precision engagement. Success will hinge on discipline, integration, continuous innovation, and the institutional willingness to adapt doctrine and training to the pace of technological change.

References

[1] "The Drone Revolution: Lessons from Ukraine," Latvian Institute of International Affairs, 2024.
[2] "Mapping the MilTech War: Eight Lessons from Ukraine's Battlefield," IFRI, February 2026.

[3] "Russia's Changes in the Conduct of War Based on Lessons from Ukraine," Military Review, September-October 2025.
[4] "Drones in the Nagorno-Karabakh War: Analyzing the Data," Military Strategy Magazine, 2022.
[5] "The Counter-UAS Conundrum," European Security and Defence, February 2026.
[6] "The Future of Air Superiority: Command of the Air in High-Intensity Conflict," IFRI, September 2025.
[7] "Drone Warfare and the Battle for the Air Littoral," CLAWS, December 2025.
[8] "Operation Allied Force: Lessons for the Future," RAND Corporation, 2001.
[9] "Campaign Analysis of NATO Ground Forces - Kosovo," DTIC, ADA381348, 2000.
[10] "Operation Anaconda in Afghanistan: A Case Study," DTIC, ADA463075.
[11] "Operation Anaconda, Shah-i-Khot Valley, Afghanistan, 2-10 March 2002," Military Review.
[12] "Iraq, 2003: Operation Iraqi Freedom," RAND, MG-405-AF.
[13] "The Invasion of Iraq 2003 - Complete Animated Documentary," YouTube Historical Archive.
[14] "Highway of Death," Wikipedia, Gulf War documentation.
[15] "Iraqi Combatant and Noncombatant Fatalities in the 1991 Gulf War," comw.org, PDA-0310RM8AP2.
[16] "Persian Gulf War | Summary, Dates, Combatants," Encyclopaedia Britannica.
[17] "Kosovo War," Wikipedia, casualty and operations data.
[18] "American Drone Strikes in Pakistan," Wikipedia, New America Foundation data.
[19] "The Drone War in Pakistan," New America Foundation.
[20] "MQ-9 Reaper Fact Sheet," U.S. Air Force, af.mil.
[21] "MQ-9A Reaper (Predator B)," General Atomics Aeronautical Systems, ga-asi.com.
[22] "The 2020 Nagorno Karabakh War: Unmanned Combat," RAF Centre for Air and Space Power Studies, ASPR Vol.25, 2023.
[23] "Turkish Drones Disrupting Battlefields: A Case Study of Karabakh," Wah Academia, 2025.
[24] "TB2 Bayraktar: Big Strategy for a Little Drone," IFRI, 2023.
[25] "FPV Drone Casualties in Ukraine: What Limited Data Suggests," Crisis Medicine.
[26] "Winning the Kill Chain Competition," Mitchell Institute for Aerospace Power, Policy Paper 40, 2023.
[27] "Find, Fix, Track, Target, Engage," Air and Space Forces Magazine, July 2000.
[28] "Shrinking the Kill Chain," Military Embedded Systems, June 2017.
[29] "C-UAS Kill Chain (F2T2EA)," The Lightning Press.
[30] "Optimizing the Air-to-Ground Kill Chain for Time-Sensitive Targets," DTIC, ADA509155, 2009.
[31] "Countering the UAS Threat: A Comprehensive Review," C-UAS Hub Market Report, 2025.
[32] "Mapping the Recent Trends in China's Military Modernisation," ORF, September 2025.