CLEARED
For Open Publication
Sep 24, 2026
Department of War
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

Joint Interagency TaskForce 401(JIATF-401)
Counter small Unmanned Aircraft Systems (C-sUAS) Fundamentals Handbook

2026

MESSAGE FROM THE DIRECTOR OF THE JOINT INTERAGENCY TASK FORCE 401 (JIATF-401)

The proliferation of small, unmanned aircraft systems (sUAS) is changing the character of warfare and creating new challenges at home and abroad. Their low cost, accessibility, adaptability, and increasing lethality allow adversaries to create effects once reserved for far more sophisticated capabilities. We see these systems employed on battlefields overseas, around critical infrastructure, along our borders, and increasingly in the airspace we are charged to protect. Countering this threat begins with understanding it.

There is no single system, technology, or tactic that solves the C-sUAS problem. Effective defense requires a layered approach that combines detection, tracking, identification, command and control, and defeat capabilities with sound planning, trained operators, appropriate authorities, and tactics suited to the mission and environment. Just as important, we must continually learn from operations, testing, exercises, and one another.

That is why JIATF-401 is committed not only to accelerating C-sUAS capabilities, but also to expanding the collective understanding of how to employ them. Technology will continue to change rapidly. The fundamentals of effective defense must keep pace. This includes understanding the threat, integrating capabilities, assigning responsibilities, rehearsing the fight, and adapting faster than the adversary.

This pamphlet contributes to that effort. It provides commanders, staffs, planners, and operators with practical considerations for planning, preparing, executing, and assessing protection operations against sUAS threats. It is intended to complement existing joint doctrine, capture lessons emerging from across the force, and provide a common foundation from which organizations can develop solutions appropriate to their missions.

Our advantage will not come from any one solution. It will come from a force that understands the problem, shares what it learns, integrates capabilities effectively, and continually improves how it operates. The threat will keep evolving, and so will we.



Matthew Ross
Brigadier General, U.S. Army
Director, JIATF-401

PREFACE

1. Purpose

This pamphlet provides the joint force with considerations for planning, preparing, executing, and assessing Counter small Unmanned Aircraft Systems (C-sUAS) operations. It addresses the unique challenges posed by Groups 1, 2, and 3 unmanned aircraft system (UAS) threats in both expeditionary and homeland defense contexts. The Joint Interagency Task Force 401 (JIATF-401) recognizes Groups 1, 2, and 3 UAS as small UAS (sUAS). Because of this distinction, even though Joint Doctrine Note (JDN) 1-26 *C-sUAS* is the primary reference for this pamphlet, this pamphlet does not refer to Groups 1, 2, or 3 UAS as "smaller" UAS.

2. Problem Statement

Current joint doctrine provides modest considerations for planning, preparing, and executing C-sUAS operations, and there is a doctrinal gap pertaining to C-sUAS operations. The proliferation of commercially available sUASs, their demonstrated lethality, and the expanding threat to the homeland demand that the joint force expand its set of considerations for commanders to counter this threat.

3. Scope

This pamphlet applies to the joint force and addresses C-sUAS operations, emphasizing operations against Group 1 through Group 3 UAS threats. It does not supersede existing joint publications (JPs) but provides additional planning considerations, operational frameworks, and guidance to fill identified doctrinal gaps. Countering Groups 4 and 5 UASs falls within the scope of existing air defense and counterair doctrine (JP 3-01, *Countering Air and Missile Threats*). However, this pamphlet acknowledges that, to be successful, C-sUAS operations must be integrated into C-UAS operations and synchronized with air and missile defense.

4. Application

The guidance in this pamphlet is not authoritative. If conflicts arise between this pamphlet and a JP, the JP takes precedence for the activities of joint forces, unless the Chairman of the Joint Chiefs of Staff provides more current and specific guidance.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

CHAPTER I
OPERATIONAL ENVIRONMENT 6

CHAPTER II
UNMANNED AIRCRAFT SYSTEM THREAT 17

CHAPTER III
ROLES AND RESPONSIBILITIES 27

CHAPTER IV
PLANNING 34

CHAPTER V
LAYERED COUNTER-SMALL UNMANNED AIRCRAFT SYSTEM DEFENSE 52

CHAPTER VI
AIRSPACE CONTROL 65

CHAPTER VII
TRAINING AND EDUCATION 77

CHAPTER VIII
FUTURE OF COUNTER-SMALL UNMANNED AIRCRAFT SYSTEMS 86

APPENDIX 88

GLOSSARY 93

REFERENCES 95

EXECUTIVE SUMMARY

a. Small, unmanned aircraft systems (sUASs) represent a significant and rapidly evolving threat to the joint force. Conflicts in Ukraine and the Middle East have demonstrated that low-cost, commercially available sUASs can fundamentally alter the offense-defense balance, enabling actors with limited resources to impose disproportionate effects on military operations. This shift is not confined to a single theater. Every combatant command faces some variant of the sUAS threat, from sophisticated, state-employed systems to commercially modified platforms operated by non-state actors and transnational criminal organizations (TCOs).

b. Modern warfare examples show that, by integrating emerging technologies and achieving interoperability, the joint force develops and maintains a decisive edge in countering the evolving threat posed by sUASs. These capabilities will enable the joint force to operate in contested environments, achieve mission success, and preserve freedom of action across all domains.

c. This pamphlet provides the joint force with a framework for C-sUAS operations organized across eight chapters.

(1) Chapter I, "Operational Environment," characterizes the operational environment and identifies trends that affect all combatant commands and the distinct challenges of homeland defense versus expeditionary operations.

(2) Chapter II, "Small Unmanned Aircraft System Threat," analyzes the sUAS threat by platform type and employment technique, drawing from observed tactics in contemporary conflicts.

(3) Chapter III, "Roles and Responsibilities," establishes roles, responsibilities, and authorities, addressing the legal frameworks that govern C-sUAS operations in both contexts.

(4) Chapter IV, "Planning," addresses planning considerations, integrating C-sUAS into the joint planning process and intelligence preparation.

(5) Chapter V, "Layered Counter-small Unmanned Aircraft System Defense," provides a layered defense framework grounded in the joint air defense kill web.

(6) Chapter VI, "Airspace Control," addresses airspace control and electromagnetic spectrum deconfliction.

(7) Chapter VII, "Training and Education," establishes the training and education framework for building joint C-sUAS readiness.

(8) Chapter VIII, "Future of Counter-small Unmanned Aircraft Systems," looks forward to emerging technologies and the expansion of the counter-uncrewed threat beyond the air domain.

CHAPTER I
OPERATIONAL ENVIRONMENT

1. Unmanned Aircraft Categorization

The unmanned aircraft (UA) categorization chart depicted below provides a basic framework to categorize UA. This chart uses max gross takeoff weight as the most crucial factor to categorize UA. However, the max gross takeoff weight range associated with Group 3 is rather large (56 - 1,320 pounds). As a result, Group 3 UA near the lower end of this range often share characteristics of Group 2, and Group 3 UA near the higher end of this range often share characteristics of Group 4.

2. Overview

a. Over the last quarter century, unmanned aircraft systems (UASs) have matured and continue to evolve. At present, their low-cost, ubiquity, and utility, especially sUASs — have altered the character of warfare. What began as a

(U) Unmanned Aircraft Categorization Chart

Category	MGTW (lbs.)	Normal Operating Altitude (ft)	Speed (KIAS)
Group 1	0 - 20	< 1200 AGL	100
Group 2	21 - 55	< 3500 AGL	< 250
Group 3	< 1320	< 18,000 MSL	
Group 4	> 1320		Any Speed
Group 5		> 18,000 MSL	

Legend

AGL	above ground level	lbs	pounds
ft	feet	MGTW	maximum gross takeoff weight
KIAS	knots indicated airspeed	MSL	mean sea level

Figure: Unmanned Aircraft Categorization Chart

state-sponsored intelligence, surveillance, and reconnaissance (ISR) capability has evolved into a versatile weapon system employed by state militaries, proxy forces, non-state armed groups, TCOs, and individuals acting alone. Improvement in UAS technology and economies of scale reduced technological and monetary barriers to entry, enabling state and non-state actors to rapidly acquire and field cutting-edge sUASs en masse. One-way attack (OWA) sUASs are ubiquitous, hard-to-counter threats to military and civilian personnel and infrastructure.

b. Small UASs can conduct varied operations. Some sUASs enable persistent surveillance, making it difficult, if not impossible, to hide force disposition and intentions from an enemy. Others can extend operational reach; shorten the sensor-to-shooter timeline (i.e., the time between acquiring a target and creating an effect); and impose social-psychological costs, such as fear, among both combatants and noncombatants. When used en masse as decoys, they can wear down air defense (AD) weapons inventories. Adversaries that develop and field new sUAS capabilities or employ new tactics can gain a temporary advantage, even against better-resourced adversaries. Lastly, the use of sUASs greatly reduces the risk to force associated with manned systems and permits an enemy to pursue riskier options, which once required personnel.

c. Counter-sUAS operations occur in the physical domains of air, land, maritime, and space; the information environment (including cyberspace); and the electromagnetic spectrum (EMS). Due to proliferation of sUASs, joint force commanders (JFCs) should synchronize actions across all domains (to include the information and electromagnetic environments) and with interagency organizations and allied and partner-nation forces.

d. Artificial intelligence (AI) has vastly improved the effectiveness of sUASs and has enhanced the ability of sUASs to operate autonomously and in swarms. A proven operational advantage exists (or is created) when employing sUASs en masse. Mass combined with precision munitions has increased the complexity of the modern battlefield. Additionally, AI algorithms, sensors, and real-time data processing have increased the precision and lethality of sUASs, especially sUASs. Artificial Intelligence provides a way to build representative data of the environment in terms of the radio frequencies (RFs) that enable adversarial sUASs to fly. This understanding provides a dynamic way to build pattern-of-life on adversarial sUASs, even when the RF enabling them is not in an existing library. Advances in AI continue to foster a new era of human-machine teaming. As these technologies mature, they calibrate the degree of human oversight to match the pace of operations, increasing the challenge of countering sUASs. The sUAS threat is defined by four converging trends.

(1) **Commercial Availability.** The global, commercial sUAS market produces millions of platforms annually that are not subject to international arms control rules or counter-proliferation frameworks. This makes them easily accessible for purchase by malign actors for a few hundred dollars in nearly every country.

(2) **Miniaturization.** Advances in battery technology, microelectronics, and sensor miniaturization have compressed significant capability into increasingly smaller airframes Platforms weighing less than one kilogram can now carry electro-optical-infrared (EO-IR) cameras, infrared sensors, or small explosive payloads at ranges exceeding several kilometers (kms).

(3) **Adaptability.** The commercial sUAS sector provides a platform that adversaries can modify with minimal technical expertise. For example, attaching an improvised explosive device (IED); a chemical, biological, or radiological dispersal mechanism; or an electromagnetic warfare (EW) payload to a commercial sUAS requires rudimentary skills and publicly available instructions. This makes it extremely easy for any actor seeking to develop an improvised capability.

(4) **Offense-Defense Imbalance.** In the past, sUASs favored the attacker over an unprepared defender. The cost to produce and employ a small attack UAS is a fraction of the cost to detect and defeat it. This disparity compounds when adversaries employ tactics such as massed or continuous attacks designed to exhaust defensive magazines and overwhelm sensor capacity. However, the balance may be shifting. The attacker still has the advantage when employing sUASs.

3. Cost-Exchange Challenge

a. By leveraging partnerships with industry, the Services can continue to develop and field lower cost sUASs. For example, the United States rapidly designed the Low-Cost Unmanned Combat Attack System, also known as LUCAS, to counter the proliferation of inexpensive, mass-produced attack sUASs like Iran's Shahed-136 or Russia's Geran-2. Priced at $35,000 per unit, this system offers a cost-effective augmentation to platforms such as the MQ-9 Reaper, which costs $30 million per unit. The Department of War's (DoW's) Defense Autonomous Warfare Group aims to acquire over 300,000 UASs in 2026, with unit costs projected to drop to $2,000 per unit. This reflects lessons learned from the Russia-Ukraine conflict, where mass sUAS swarms overwhelmed ADs and resulted in the expenditure of high-cost AD weapons.



Low-Cost Unmanned Combat Attack System (LUCAS)

b. The joint force can defeat the sUAS threat in multiple ways: Prioritizing prior-to-launch engagement by destroying the sUAS factory or intercepting the sUASs prior to their arrival to the operator or targeting the operator(s). Using non-kinetic fires (e.g., EW jamming the navigation or communication systems). Using kinetic fires against the sUAS. When possible, use the cheapest possible means to defeat the enemy. For example, use directed energy (DE) (e.g., lasers, instead of missiles). Do not unnecessarily use exquisite weapons (e.g., a Patriot) against a lower-level threat (e.g., a Shahed). Integrating passive defense measures (e.g., camouflage, concealment, dispersion, hardening) to reduce the number of engagements required.

4. Homeland Defense and Overseas Operating Environments

Countering sUASs differs between homeland and overseas environments, due to differing command and control (C2), legal authorities, coordination requirements, and operational restraints.

a. **The Homeland.** In the homeland, C-sUAS operations are governed by Title 10, United States Code (USC) (§130i), which authorizes the Secretary of War (SecWar) to

mitigate sUAS threats to covered facilities and assets within the United States. Covered facilities are designated by SecWar and are limited to those facilities and assets directly related to DoW missions specified in §130i. Counter-sUAS actions in the homeland are coordinated with the Federal Aviation Administration (FAA), Department of Homeland Security (DHS), Department of Justice (DoJ), and state and local law enforcement. The DoW may provide C-sUAS support to federal, state, local, and territorial authorities when requested. The operational area (OA) for the homeland is defined by rules for the use of force in proximity to civilian populations and infrastructure. The OA is also bound by the requirement to operate within FAA-controlled airspace rules.

1. The homeland can be a contested environment with sUAS threat influencing all domains and types of operations. Adversaries may exploit force protection gaps to collect target and degrade state, local, tribal, and territorial (SLTT) and military capabilities. Small UAS threats may interfere with daily commercial operations and activities. At the same time, adversaries may confound the military's ability to mobilize, deploy, and project forces. Using sUASs, malicious actors may seek to disrupt, degrade, delay, and even destroy core assets to deny essential and enabling capabilities.

2. In the Homeland, sUASs can be used by terrorists, criminal organizations (including transnational organizations), and lone actors to achieve specific objectives. Small UASs have been weaponized and are used by adversaries in multi-mission roles. Examples from FAA and Department of Homeland Security DHS include:

(a) **Drug Smuggling:** Cartels are known for using sUASs to smuggle drugs across borders and ISR operations to identify Customs and Border Protection (CBP) field checkpoints and foot patrols.

(b) **Prison Contraband:** Numerous prisons have reported sUASs being used to smuggle contraband such as cellphones, drugs, and weapons to inmates.

(c) **Domestic Terrorism:** Terrorist organizations could use a sUAS as a weapon system with a mission payload using homemade/improvised munitions that can be dropped from above or as an airborne guided bombs/claymore type device.



Figure. Examples of SUAS with Weapon System Payload currently in use by terrorist organizations

(d) **Flight Safety/Hazards to Flight Operations:** Numerous airports have reported sUASs that have impacted operations.

b. **Overseas Environments.** In permanent and overseas environments, combatant command authorities, theater rules of engagement (ROE), status-of-forces-agreements (SOFAs), and host nation (HN) coordination requirements govern C-sUAS operations. Commanders have broader authorities to detect, track, identify, engage, and defeat sUAS threats but face different challenges, including the integration of C-sUAS operations with ongoing combat operations, electromagnetic spectrum (EMS) congestion, and the need to distinguish between enemy sUASs and friendly or neutral commercial systems.

c. **Counter-sUAS Security Assets Within the Threat Environment by Combatant Command (CCMD) Area of Responsibility (AOR)**

(1) **USNORTHCOM [United States Northern Command] AOR.** United States Northern Command faces the unique challenge of defending the homeland against sUAS threats under domestic legal authorities. The primary concern is protection of military installations, critical defense infrastructure, and national security assets within the United States, its territories, and possessions. The threat ranges from state-sponsored intelligence collection against sensitive facilities to TCO employment of sUASs for surveillance and payload delivery along the southern border. United States Northern Command coordinates C-sUAS operations with the DHS, USCBP, the Federal Bureau of Investigation (FBI), the FAA, and state and local law enforcement under established interagency frameworks. For C-sUAS operations, military forces operate under the authorities legally available under their chain of command, pursuant to their status. In addition, military forces in the United States and its providences and territories operate pursuant to Title 10, USC (§130i), authorities. However, National Guard forces in a Title 32 or state active-duty status would operate pursuant to authorities were legally available to their state governor.

(a) **The C-sUAS situation along the US southern border:** Threat actors operating along the US-Mexico border increasingly turn to sUASs to collect information, conduct reconnaissance, and execute surveillance against US military, US Border Patrol (USBP) agents, and other law enforcement personnel. They also utilize sUAS in support of narcotics and human smuggling. Moreover, threat actors' sUAS TTPs are rapidly evolving. There are open-source reports of cartels embedding with Ukrainian units to bring back their TTPs. This situation is not simply the introduction of new technology onto the battlefield, but rather a seismic shift in small unit tactics and information collection capabilities that will reverberate through all facets of military decision making and operational planning.

1. To counter this evolving threat, JTF-SB has employed an integrated detection and response framework with interagency partners. For threat sUAS mitigation, a layered approach was used consisting of various radars, radiofrequency (RF) sensors, as well as both kinetic and non-kinetic C-sUASs. These capabilities have enabled forces to mitigate threat sUAS in self-defense under the Standing Rules for the Use of Force (SRUF). This has been conducted alongside interagency partners across DoW, DHS, and local law enforcement. The interagency nature of this mission has paralleled the integration of a future joint fight while introducing many related challenges of different organizations operating concurrently.

2. Despite the close working relationship between the DoW and USBP, there have been critical bottlenecks in information sharing and interoperability due to fragmented data transmissions among sensors, shooters, and classification domains that have impeded greater interoperability between the DoW and DHS. These constraints have significantly impeded the ability to gain situational understanding of the air domain across all levels. Without situational understanding—or even situational awareness—effective control of the air domain cannot be maintained, prohibiting the achievement of full operational control over the Southern Border.

(a) **The C-sUAS situation along the US northern border:** The small sUAS threat along the U.S.–Canada northern border has centered primarily on cross-border illicit trafficking, surveillance of law enforcement assets, and incursions near critical defense or maritime infrastructure. Counter-sUAS operations have relied on integration of DHS components, bi-national coordination with Canada, and USNORTHCOM homeland defense frameworks.

(b) **The C-sUAS situation along the US eastern and western borders:** The sUAS threat along U.S. eastern, western, and coastal borders has primarily stemmed from illicit surveillance, scouting, maritime smuggling, and potential intelligence/reconnaissance probes targeting critical infrastructure and military installations. United States Northern Command, USCBP, and the US Coast Guard (USCG) have countered these threats through integrated radar feeds, RF defeat mechanisms, directed-energy pilot programs, and layered maritime domain awareness.

(2) **United States Central Command (USCENTCOM) AOR**

(a) Iranian-produced and supplied OWA sUASs, commercially modified reconnaissance and attack platforms employed by proxy forces, and an increasing volume of semi-autonomous systems define the theater threat. Operations in Iraq, Syria, Jordan, Israel, and the broader Arabian Gulf region have required continuous C-sUAS defense of forward operating bases, logistics nodes, and naval vessels. The Houthi campaign in the Red Sea demonstrated the integration of sUASs with larger unmanned and manned systems in coordinated attacks against maritime targets. United States Central Command forces have accumulated significant operational experience with C-sUASs, including EW, kinetic interceptors, and DE prototypes, generating lessons learned that inform joint doctrine.



Figure. Drawing of Shahed-136 Drone



Figure. Mobile Carrier for Shahed-136 Drones

(b) United States Central Command have been validating lessons learned from Operation EPIC FURY and Red Sea operations against Houthi sUAS threats.

(c) United States Central Command can provide specific operational requirements for the following theater-unique considerations:

1. Iranian OWA sUAS employment patterns and tactics observed across Iraq, Syria, Jordan, and the Arabian Gulf, including Shahed-136/Geran-2 variants and their derivatives (jet-engined).

2. Proxy force sUAS capabilities and employment techniques, including Kata'ib Hezbollah, Harakat al-Nujaba, and other Iran-backed militia groups operating across Iraq, Jordan, and Syria.

3. Houthi sUAS integration with anti-ship ballistic missiles (BMs), cruise missiles, and naval mines as part of a multi-layered, anti-access strategy in the Red Sea and Bab el-Mandeb Strait.

4. Maritime C-sUAS requirements for naval forces operating in confined waters, including the Red Sea, Arabian Gulf, Strait of Hormuz, and Gulf of Oman, where maneuver space is limited and commercial traffic is dense.

5. Integration requirements for coalition and partner C-sUAS capabilities and information-sharing protocols with Gulf Cooperation Council nations and other regional partners.

6. Counter-Shahed-specific tactics, techniques, and procedures (TTP) validated through operational experience, including EW employment, kinetic fires effectiveness, and mobile firing team integration.

7. Forward operating base and cooperative security location defense requirements against massed sUAS attacks, including Al Asad Air Base, Al Tanf Garrison, and other locations that experienced sustained sUAS campaigns.

8. Continuous adaptation requirements recognizing that enemy sUAS modifications occur in 2-to-4-week cycles, requiring rapid doctrinal and tactical

updates.

9. Cost-exchange considerations specific to theater operations, where multi-million-dollar interceptors have been employed against low-cost OWA sUASs.

10. Prior-to-launch targeting procedures for Iranian sUAS production facilities, supply routes through Iraq and Syria, and proxy force assembly areas.

11. Electronic Warfare prioritization based on operational effectiveness rather than non-interference, reflecting lessons learned from the 04 MARCH 2026 "C-sUAS Lessons Learned Conference – USCENTCOM Takeaways."

12. Integration of low-cost acoustic sensors providing critical early warning at air ingress points, addressing the responsibility gap between AD and EW organizations.

13. Mobile firing team employment providing low-cost, high-impact AD solutions for forward operating base defense.

14. All C-sUAS and shooter integration into a single C2 platform with robust EW deconfliction capability to prevent fratricide.

15. Speed of signal analysis and jamming technique development as decisive factors in the C-sUAS fight, requiring rapid adaptation to enemy counter-countermeasures within operationally relevant timelines.

(3) **United States European Command (USEUCOM) AOR.** United States European Command faces the sUAS threat from two different contexts. First, USEUCOM's ability to defend operating locations to generate multi-domain operations in support of USCENTCOM (e.g., Operation EPIC FURY). Second, a contested European security environment shaped by the Russia-Ukraine conflict.

(a) The Russian Armed Forces have added an unmanned security force to their structure that engages in the conflict daily. The war in Ukraine has generated extensive operational data on sUAS employment and C-sUAS operations in modern warfare, including massed first-person view (FPV) sUAS attacks, autonomous target recognition, fiber-optic-controlled systems resistant to EW, and industrial-scale sUAS production.



Figure. Upyr-10 Russian FPV Kamikaze Drone



Figure. KVN Russian FPV Kamikaze Drone

(b) While US forces are not engaged, the lessons from this conflict inform USEUCOM theater defense planning, North Atlantic Treaty Organization (NATO) interoperability requirements, and the forward positioning of C-sUAS capabilities to defend alliance installations. To further support and apply such learning, the United States Army has established two UAS labs in the region to create, test, and apply UAS results to frontline capabilities.

(c) Russia remains a threat to US forces, allies, and partners, although currently engaged in Ukraine. Russian sUAS training is changing from being conducted by volunteer services with no overarching course work to a more structured program associated with the formation of the UAS troops organization. Training lasts about 3-4 weeks. Lesson plans typically include acquisition, targeting, EW capabilities, and the structure of specific sUASs. Some courses teach operators how to assemble sUASs and use simulators prior to flight time.

(d) **Integration with Theater BM Defense.** Counter-sUAS operations integrate with theater BM defense systems when defending strategic assets. This includes:

1. Coordination requirements, which include common operational picture (COP) development, engagement zone deconfliction, and prioritization of combined sUAS with missile threats.

2. Counter-sUAS defense of BM defense sites, which require integration with site-organic sensors (e.g., AN/SPY-1 radar) and coordination with HN territorial defense forces.

3. Maritime approaches to BM defense sites, which require monitoring for sea-launched sUAS threats as well.

(e) **Host Nation (HN) Air and Missile Defense (AMD) Coordination Requirements.** In theaters with HN AMD capabilities, C-sUAS operations require coordination through established mechanisms, including:

1. Integration with HN air operations centers and deconfliction with HN AD systems.

2. Liaison officers embedded in theater and HN air operations centers enabling real-time coordination.

3. Coordination with HN territorial defense missions, particularly for forces lacking organic, medium-range AD requiring the US C-sUAS to provide operational-level coverage.

(4) **United States Africa Command (USAFRICOM) AOR.** United States Africa Command recognizes the serious and growing threat posed by sUASs in its AOR. The command has identified countering violent extremist organizations as its top priority. Key concerns include threats to US personnel and facilities in Africa. Al-Shabaab has a history of attacking US personnel. The proliferation of sUASs contributes to instability in regions already grappling with conflict and weak governance, such as the Sahel, which has been described as the epicenter of terrorism. United States Africa Command is particularly concerned about the potential for collaboration between groups like the Houthis and al-Shabaab, which could significantly increase the threat to maritime security and regional stability.

(5) **United States Pacific Command (USPACOM) AOR.** United States Pacific Command faces a sUAS threat set defined by the People's Republic of China's advanced sUAS development and the vast maritime distances of the Indo-Pacific theater. The People's Republic of China fields a sophisticated domestic sUAS industry that produces both military and commercial sUASs and exports these systems globally. In a potential conflict scenario, the joint force would face sUAS threats to forward-deployed forces across island chains, naval formations, and logistics nodes spread across thousands of miles of ocean. The maritime dimension adds complexity to the detection of low-flying sUASs over water, defense of dispersed expeditionary forces, and EMS management across distributed formations that present unique C-sUAS challenges not fully informed from land-centric operational experience. While conducting C-sUAS operations as part of homeland defense, USPACOM defends US territories under domestic C-sUAS authorities. Finally, the United States Army established two UAS labs in the region to design, manufacture, and test UASs locally, to include for use in jungle environments.

(6) **United States Southern Command (USSOUTHCOM) AOR.** United States Southern Command faces a sUAS threat primarily from criminal organizations. Drug trafficking organizations have employed sUASs for counter-surveillance against law enforcement, attacks on the police and military, and increasingly for cargo delivery. While the current threat is less militarily sophisticated than those faced by USCENTCOM or USEUCOM, the trend lines indicate growing capability and willingness to employ sUASs in ways that threaten US personnel, partner-nation security forces, and cooperative security locations. United States Southern Command C-sUAS requirements focus on force protection for security cooperation missions, intelligence collection on criminal sUAS capabilities, and support to partner-nation C-sUAS capacity building.

5. Risks, Limitations, and Mitigation Strategies

Joint Force Commanders (JFCs) and their staff weigh risk, consider limitations, and develop mitigation strategies for each operation and threat environment. Counter-sUAS operations have specific factors that JFCs and their staff should consider. For an overview of risks, limitations, and mitigation strategies, see Appendix, "Risks, Limitations, and Mitigation During Counter-small Unmanned Aircraft System Operations."

CHAPTER II
SMALL UNMANNED AIRCRAFT SYSTEM THREAT

The use of UASs, particularly sUASs, is a continuous and evolving threat to the joint force and its partners. As of the publishing date of this pamphlet, state and non-state actors operate over 600 different sUAS models across more than 80 countries. When integrated with fires and ISR capabilities, they constitute a significant threat to the joint force. The increased use of sUASs to target friendly forces and weaken public resolve demonstrates that sUASs are an enduring threat.

1. Small Unmanned Aircraft System Sourcing, Communication, Navigation, and Autonomy

a. **Small UAS Sourcing Strategies.** Small UASs are sourced in three primary ways—purpose-built, commercial off-the-shelf (COTS) systems, or hybrid approach.

(1) **Purpose-built** systems meet explicit military specifications. This optimizes their performance, survivability, and interoperability for specific missions. However, these specialized systems are usually expensive. Additionally, they often require lengthy development and production cycles.

(2) **Commercial off the Shelf (COTS)** systems offer significant acquisition advantages. They are commercially developed and procured from existing markets. This makes them affordable and readily available for rapid deployment. The democratization of technology accelerates COTS proliferation through global supply chains.

(3) A **hybrid approach**, known as militarized COTS, also sees frequent use. This involves adapting commercial platforms for military tasks. For example, operators can modify a COTS sUAS for weapons employment. This sourcing strategy balances cost with the speed and scale offered by commercial technology. It has become a defining feature of modern conflicts.

b. **Communications**

(1) Small UAS operations rely on various communication links. These links facilitate the flow of information. The four primary types are UA-to-UA, UA-to-base, UA-to-repeater, and UA-to-spacecraft. Within these links, four distinct channels carry specific information. The C2 channel sends directions to the sUAS. The telemetry channel transmits aircraft status back to the operator. A position, navigation, and timing channel provides location data. Finally, the sensor channel sends environmental data to the ground control station. These channels are often bundled into a single frequency band for transmission.

Operators employ various UA-to-base communication links for sUAS control. Radio Frequency links remain the most common method. They provide reliable line-of-sight (LOS) control over moderate distances. However, RF signatures remain vulnerable to enemy EW. To mitigate this, operators use fiber-optic cables for tethered control. Fiber- optic links eliminate electromagnetic emissions entirely. This ensures secure, un-jammable communications in contested environments at the cost of range.



Figure. Fiber-Optic Drone, Showing Fiber-Optic Spool and Line

(2) Cellular UA-to-base links utilize existing commercial network infrastructure. This approach offers extended range without dedicated military satellites. Advanced systems increasingly utilize networked UA-to-UA communication architectures. An example of this is a MANET [mobile ad hoc network], which represents a critical evolution. Radio frequency-enabled MANETs link multiple sUASs together directly. Each sUAS functions as a node within a mesh network. They relay data to one another seamlessly across the OA. This decentralized structure enhances overall system resilience. If an enemy destroys one node, the network immediately self-heals. Mobile ad hoc networks facilitate complex swarm tactics and collaborative autonomous operations and reduce reliance on vulnerable centralized control nodes.

(3) Not all sUAS operations require constant communication links. Many platforms maintain strict electromagnetic silence to evade enemy detection. Operators pre-program flight paths using Global Navigation Satellite System (GNSS) waypoints. The aircraft navigates to an initial point without transmitting data. Upon arrival, the sUAS activates its C2 and sensor channels. Operators then assume FPV control to conduct detailed ISR collection. Alternatively, OWA sUASs can strike without ever emitting signals. This deliberate emission control severely complicates RF countermeasures.

c. **Autonomy and Automation.** Autonomy and automation are distinct but related concepts. Automation is the mechanization of specific tasks. Autonomy is the system's ability to operate and make independent decisions.

(1) Department of War (DoW) uses a five-level scale to characterize UAS autonomy. Levels range from 0 (human-operated) to 4 (full autonomy). Lower levels (0-1) rely on rule-based responses to known situations. Higher levels (3-4) employ dynamic responses for unknown situations. Mid-level autonomy (2) blends both response types. This progression allows for increasingly complex and independent sUAS operations.

(2) These autonomy levels directly correlate with sUAS control methods. At lower levels (0-2), a human directly controls the aircraft. This control is maintained via RF, fiber-optic, or cellular network links. The system may automate tasks like following a pre-programmed route, but a human remains in or on the loop, ready to intervene. At higher levels (3-4), the system operates with full autonomy with AI-driven sUASs using

advanced target recognition to make decisions. They collaborate using UA-to-UA mesh networks to achieve objectives without human intervention. This represents true human-out-of-the-loop capability.

d. **Navigation.** Small UAS navigation methods align closely with their respective autonomy levels, as illustrated in the Unmanned Aircraft System Navigation and Control Matrix Figure. At Level 0, operators primarily use FPV. This requires constant human input for basic flight control. Levels 1 and 2 introduce automated navigation techniques. Systems follow pre-programmed GNSS waypoints using inertial navigation systems for dead reckoning. Inertial navigation systems allow continued flight in GNSS-denied environments. Levels 3 and 4 feature advanced, highly autonomous navigation. These systems employ optical sensors and terrain matching algorithms. This enables independent navigation without external satellite signals.

Unmanned Aircraft System Navigation and Control Matrix

Autonomy Level	Navigation Method	Primary Control & Communications	Human Involvement
Level 0	First-Person View	RF, Fiber-Optic, Cellular	In-the-Loop (Constant Input)
Levels 1-2	GNSS Waypoints, INS (Dead Reckoning)	RF, Fiber-Optic, Cellular	On-the-Loop (Ready to Intervene)
Levels 3-4	Optical/Terrai n Matching	AI-Controlled, Mesh Networks	Out-of-the-Loop (Independent)

Legend
AI artificial intelligence
GNSS Global Navigation Satellite System
INS inertial navigation system
RF radio frequency

Figure. Unmanned Aircraft System Navigation and Control Matrix

2. Small Unmanned Aircraft Operations, Payloads and Effects, and Countermeasures Operations

a. Small UAS Operations

(1) Small UASs have fundamentally transformed current military operations with commanders deploying them across a broad spectrum of missions. Initially, militaries used sUASs primarily for ISR. Today, these systems execute complex, multi-role mission profiles, to include EW, kinetic strike, and tactical resupply. Furthermore, sUASs serve as essential force multipliers in the area of operation. Militaries use low-cost, expendable sUASs to protect high-value manned assets. This strategy reduces risk to human operators while expanding operational reach.

(2) Modern operations network sUASs into a comprehensive kill web replacing traditional, linear kill chains. Within this web, individual sUASs function as distributed sensor or shooter nodes, identifying targets and rapidly sharing tactical data across the formation. This seamless integration drastically reduces the sensor-to-shooter timeline, enabling commanders to engage targets with unprecedented speed and precision. Swarming tactics further complicate enemy defenses with multiple sUASs coordinating their actions to overwhelm enemy AD systems.

(3) This lethal paradigm drives the development of specialized combat sUASs, such as OWA sUASs for precision strikes. Many OWA sUASs utilize GNSS waypoints for silent, autonomous infiltration. Operators also guide reusable bomber sUASs dynamically via Level 0 FPV links. This human-in-the-loop interaction ensures accurate munition delivery on mobile targets. For covert ISR, operators actively employ strict emission control tactics to enable silent navigation to an initial point before transmitting data. Advanced forces also develop Level 4 loyal wingman platforms. These semi-autonomous jets fly alongside manned fighters providing commanders with scalable, networked strike options.

b. **Payloads and Effects**

(1) **Payloads.** A sUAS's payload is the equipment it carries to perform a mission. For ISR missions, sUASs employ sophisticated sensor payloads. Electro-optical cameras provide high-resolution daytime imagery. Infrared sensors offer thermal imaging for nighttime operations. These visual sensors allow operators to detect and track enemy activity. Other platforms carry signals intelligence (SIGINT) payloads. These specialized receivers intercept and locate enemy communications. This provides commanders with critical intelligence on enemy intentions and dispositions. These ISR payloads enable persistent surveillance of the OA.

(2) **Effects.** Military planners categorize combat payloads and countermeasures using a two-by-two matrix (see Figure below). This framework strictly separates the delivery method from the final outcome. Methods are either kinetic, using physical force, or non-kinetic, using electromagnetic energy. Outcomes are either lethal, causing permanent destruction, or nonlethal, causing temporary disruption. This distinction ensures commanders match the correct capability to their desired tactical effect.

(3) Defending against sUASs requires layered C-sUAS strategies. Defenders directly apply the method-and-outcome matrix to categorize these defensive systems. Kinetic fires options physically destroy incoming sUASs using projectiles or direct ramming. Kinetic fires that employ nonlethal systems safely neutralize threats by entangling aircraft in nets. Non-kinetic fires instantly burn internal electronics to destroy the UA. Finally, non-kinetic fires that employ nonlethal methods disrupt enemy operations without destroying the platform. Defenders routinely jam command links, spoof GNSS signals, or dazzle optical sensors. Furthermore, passive defenses like hardening, camouflage, and concealment degrade enemy targeting.

Delivery Method	Desired Outcome	System Application	C-sUAS Example
Kinetic	Lethal	Physical destruction of the target using mass or explosives.	Projectile systems (guns), kinetic intercept (ramming), loitering munitions.
Kinetic	Non-Lethal	Physical interference without causing permanent destruction.	Net capture systems.
Non-Kinetic	Lethal	Permanent destruction of critical electronic components using directed energy.	High-Power Microwave, High-Energy Laser, Electromagnetic Pulse.
Non-Kinetic	Non-Lethal	Disruption, deception, or degradation of enemy systems.	Laser dazzling, C2/GPS jamming, spoofing, hijacking, decoys.

Figure. Capabilities and Effects Matrix

3. Small Unmanned Aircraft Systems—Enemy System-of-Systems

a. To counter sUASs, it is important to understand the flight mode—manual, semi-autonomous, autonomous, and FPV sUASs.

(1) **Manual Mode.** In manual mode, the operator flies the sUAS without a preprogrammed flight plan. The operator views the UA directly or utilizes an onboard sensor package. The UA may display more erratic flight characteristics using this flight mode.

(2) **Semi-Autonomous.** In semi-autonomous mode, the UA acts independently to some degree but still requires pilot input for specific operations such as selection of a minimum or maximum altitude for the flight or providing the UA with control to manage distance, direction, and speed.

(3) **Autonomous.** An autonomous mode is a preprogrammed flight mode for the sUAS with no live input from the pilot/operator. This includes the ability to fly hands free and enables computer-controlled flight with preprogrammed missions. This mode will have a smoother, fixed flying path and transitions when turning to its next waypoint. The sUAS may make in-flight self-corrections without operator intervention to stay on mission.

(4) **FPV sUAS.** An FPV sUAS is equipped with a video camera and transmits real-time images to the pilot's goggles or helmet (controlled in the first person).

b. Regardless of the mode, analyzing the nodes within the system enables the determination of critical vulnerabilities for targeting and protection. Most sUASs require all nodes to function properly for the UA to successfully perform its function and have the following nodes: UA, operator(s), ground control station, launch and recovery infrastructure, communication architecture and data link, or remote-control mechanism.

Despite physical differences across UA, such as size, altitude, speed, and payload capacity, all sUASs have a common characteristic—they do not have a pilot physically on board.



Figure. First Person View (FPV) Operator and Drone

c. **System Nodes.** To counter sUASs, it is important to understand the various nodes that enable UASs to operate. Each of these nodes represent a potential critical vulnerability. Attacking these vulnerabilities can create effects within the entire enemy system.

(1) **UA.** The UA is the airborne platform that houses the payload such as a warhead, SIGINT package, EW package, or full-motion video camera. The UA has certain flight performance characteristics such as max gross takeoff weight, endurance limitations, maximum airspeed, and maximum operating ceiling. Environmental conditions, such as fog, clouds, or high winds, can limit, or completely restrict, a UA from flying or performing its function. The UA may have sophisticated countermeasures or may have no countermeasures at all. Understanding the capabilities and limitations of the UA enables optimum weapon-to-target-matching to neutralize or destroy the UA.

(2) **Operator(s).** The type and sophistication of the UA often determine the degree of training and skill required to operate it. Larger and more sophisticated UA often require a certified pilot, while small, expendable UA may be operated by someone with limited or rudimentary training. Additionally, the degree of system input by the operator can vary. UA with limited, or no, automation may require constant input by an operator, while more sophisticated UA may require minimal input from an operator or be preprogrammed so there is no operator input during flight. Essentially, the degree of sophistication and automation determines whether the operator is in-the-loop (i.e., operator is actively involved in the decision-making process, provides inputs, approves actions) or on-the-loop (i.e., operator supervises the system, monitors actions, intervenes only if the system fails or makes an error). Lastly, the type of UA often dictates the proximity of the operator relative to the UA. Pilots can control larger and more sophisticated systems from thousands of miles away, while small and less sophisticated systems may require an operator to be within several kms of the UA to maintain LOS. The location of the system operator, and the degree of their required input, may permit the commander to target the operator or suppress the operator's ability to perform their role, thus limiting or preventing them from successfully controlling the UA.

(3) **Ground Control Station or Remote-Control Mechanism.** The system operator requires a ground control station or remote-control mechanism to communicate with and control the UA. Pilots may use a hand-held tablet to control small and less-sophisticated UA. In some instances, the control mechanism may be an integral part of an existing platform. For instance, a manned, fixed-wing, or rotary-wing platform may be designed to fly alongside and control a UA, often referred to as a manned-unmanned teaming. Depending on the location and degree of physical or cyberspace protection, the ground control station or remote-control mechanism may be vulnerable to attack. Commanders may choose to target the physical control apparatus, rendering the system operator incapable of controlling the UA.

(4) **Launch and Recovery Infrastructure.** The type of UA determines the method of launch and recovery. Larger UA often require a runway to launch and recover, along with dedicated ground crew and systems designed to control the vehicle during takeoff and landing. Small UA may require a mechanism to initially propel the UA into the air (e.g., pneumatic or mechanical spring launch mechanism). Recovery of these UA may be via an apparatus such as a parachute, net, or hook and cable system. Small UA may take off and land without any support equipment or may be small enough for operators to physically throw them into the air. Understanding the launch and recovery infrastructure enables the commander to potentially target the infrastructure and render the UA inoperable.

(5) **Communication Architecture and Data Link.** Most UA require some form of communication architecture to enable the system operator to control the UA and any onboard payloads, as well as receive telemetry data and full-motion video. UA often rely on the EMS to establish communication with the system operator or with a position, navigation, and timing source. Typically, operators control UA by RF, cellular networks, or fiber-optic cables. RF control requires either BLOS [beyond line-of-sight], LOS satellite communication, or LOS VHF [very high frequency]/UHF [ultrahigh frequency]/SHF [super-high frequency]. These systems also employ various antenna configurations (e.g., omnidirectional, directional) and communication technology (e.g., frequency-hopping, spread-spectrum, frequency-switching). Additionally, these systems can leverage VPNs [virtual private networks] to mask their location. The linkages between the UA and the system operator or position, navigation, and timing source connection are vital for the employment of the UA. Understanding this linkage and the inherent vulnerabilities provide options to disrupt or sever this linkage for all UA relying on the targeted linkage. This may permit multiple effects by targeting a single portion of the EMS vice targeting each individual UA. The ability to identify, target, and sever a link may become increasingly challenging as AI is able to assist inertial navigation systems or terrain mapping navigation which may allow the UA to navigate to, and attack, its intended target without the requirement for a communication link with the operator.

(6) **Sustainment.** The sUAS threat is not bound to the tactical level of warfare but rather is a complex system-of-systems that includes multiple supply chains. This system-of-systems fulfills critical requirements, providing fuel, munitions, maintenance, and repair services enabling sUAS operations. As such, disruption of these sustainment systems, such as by physical attack, cyberspace attack, or irregular warfare means, can severely degrade the enemy's ability to use UASs.

4. Small Unmanned Aircraft Systems Employment Techniques

Enemy sUAS employment techniques vary by actor, theater, and objective, but contemporary conflicts have generated a body of observed tactics that inform joint C-sUAS planning. The following summarizes key employment patterns from current and recent operations.

a. Ukrainian versus Russian TTP

(1) The Russia-Ukraine conflict represents a data-rich operational laboratory for sUAS employment and C-sUAS operations. Both sides employed tens of thousands of sUASs monthly for reconnaissance, direct attack, artillery adjustment, and EW missions.

(2) Ukrainian forces pioneered the use of commercial FPV sUASs as precision strike platforms against Russian armored vehicles, logistics convoys, and personnel. Ukrainian employment emphasized operator skill, decentralized execution, and rapid adaptation to Russian EW. When Russian jamming degraded RF and GNSS-based control, Ukrainian forces shifted to fiber-optic-controlled systems and AI-assisted terminal guidance to maintain attack effectiveness.

(3) Russian forces employed sUASs for reconnaissance, artillery adjustment, and direct attack using Lancet loitering munitions and modified commercial platforms. Russian employment emphasized integration ofs UAS reconnaissance with artillery fires, using sUASs to locate targets and observe the effects of strikes in near real time. Russian EW capability is extensive, and units deployed area and point-jamming systems designed to deny GNSS and disrupt commercial sUAS control links.

(4) Both sides developed massed attack techniques, launching multiple small UASs simultaneously or in rapid sequence to overwhelm defensive systems. Continuous attack, where waves of sUASs are launched over extended periods to exhaust defensive magazines and degrade operator alertness, was a defining characteristic of the conflict.

b. Israeli Versus Iranian TTP

(1) The Israel-Iran confrontation encompassed both direct Iranian sUAS employment and proxy force operations by Hezbollah, Hamas, the Houthis, and Iran-backed Iraqi militia groups. This multi-front threat environment demonstrates the integration of state-level sUAS capabilities with proxy force operations, creating a distributed threat network that spans multiple theaters and employs diverse TTP.

(2) Iranian-produced OWA sUASs, including variants of the Shahed-136/Geran OWA sUAS, have been employed in massed attacks against Israeli territory and against US and multinational forces in Iraq and Syria. Iranian employment doctrine emphasizes saturation, launching large numbers of low-cost OWA UASs alongside BMs and cruise missiles to overwhelm AMD systems. The April 2024 Iranian direct attack on Israel employed over 300 munitions, including OWA UASs, BMs, and cruise missiles in a coordinated salvo designed to exhaust defensive interceptor magazines and create windows of vulnerability for follow-on strikes. Subsequent Iranian attacks have demonstrated continued refinement of this layered approach, with increasing emphasis on timing coordination between sUAS and missile salvos to maximize defensive complexity.

Iranian forces have adapted their employment based on observed AMD responses, adjusting launch timing, approach corridors, and munition mix to exploit identified defensive seams.

(3) Houthi forces in Yemen employed Iranian-supplied and domestically modified sUASs against maritime targets in the Red Sea, commercial shipping, and Saudi Arabian infrastructure. Houthi employment demonstrates the integration of sUASs with anti-ship BMs and naval mines as part of a multi-layered, antiaccess strategy designed to deny freedom of navigation in the Bab el-Mandeb Strait and southern Red Sea. Houthi forces have demonstrated adaptive employment, modifying attack profiles based on observed C-sUAS effectiveness and shifting between reconnaissance, harassment, and direct attack missions to maintain operational pressure on maritime forces.

(4) Hamas and Hezbollah have employed sUASs for reconnaissance of Israeli positions, direct attack, and attempted infrastructure disruption. Hamas employment during recent conflicts has focused on small, commercially available platforms modified to carry IEDs for attacks against Israeli border positions and civilian infrastructure. Hezbollah has demonstrated more sophisticated UASs, including longer-range reconnaissance platforms and explosive-laden systems employed against Israeli AD positions and C2 nodes. Both organizations have adapted their tactics based on Israeli C-sUAS responses, including increased use of decoy UASs to identify defensive positions and employment of multiple simultaneous launches to complicate Israeli engagement prioritization.

(5) The proxy force employment model demonstrates several operationally significant characteristics. Iranian advisors provide technical training, operational planning support, and system maintenance expertise to proxy forces, enabling capability transfer while maintaining strategic deniability. Proxy forces adapt Iranian-provided systems to local operational requirements, modifying commercial platforms and integrating locally fabricated payloads. The distributed nature of proxy force operations complicates prior-to-launch targeting, as launch sites, assembly areas, and operator networks are dispersed across multiple countries and often co-located with civilian populations. Intelligence preparation should address the entire proxy force sUAS network, from Iranian production and supply routes through regional distribution nodes to tactical employment cells.

c. **Small UAS TTP Adaptation**

(1) **Exploiting Enemy Small UAS Training Deficiencies.** There are exploitable vulnerabilities in enemy sUAS operator training.

(a) **Non-State Actors TTP.** Non-state actors such as transnational criminal organizations (e.g., Central American drug cartels) and foreign terrorist organizations (e.g. ISIS [Islamic State of Iraq and Syria], al Shabaab) have adopted commercial sUASs for surveillance, counter-surveillance, and payload delivery. Cartel sUAS employment includes reconnaissance of law enforcement and military positions, monitoring of rival cartel movements, delivery of narcotics across the United States-Mexico border, and weaponized sUAS attacks against rival organizations and security forces. Cartel platforms were predominantly COTS quadcopters, but the sophistication of employment is increasing. The cartel sUAS threat is relevant to USNORTHCOM and USSOUTHCOM operational planning because it represents a non-state, non-military

enemy employing sUASs in proximity to US territory and personnel. With the resources available to these cartels, it is easy to imagine them weaponizing them to further their interests.

CHAPTER III
ROLES AND RESPONSIBILITIES

1. Authorities

a. **During Homeland Defense: The United States, its Territories, and Possessions**

(1) Multiple overlapping legal authorities govern C-sUAS operations within the United States, its territories, and possessions. The primary DoW authority is Title 10, USC (§130i), which authorizes SecWar to take actions to mitigate sUAS threats to covered facilities and assets. Covered facilities are those identified by SecWar as directly related to specific DoW missions, including nuclear deterrence, missile defense, and national security space. Authorized actions include detection, identification, monitoring, tracking, warning, and mitigation of sUAS threats, including the use of reasonable force to disable, damage, or destroy the sUAS.

(2) National Guard forces operating under Title 32, USC, authority can only provide C-sUAS capability pursuant to authorities legally available to their chain of command (i.e., their state governor). National Guard state active-duty operations are directed by the state governor through the adjutant general. When National Guard members are in a state active duty or Title 32 duty status, they are not members of the armed forces – as such, Title 10, USC (§130i), authorities and protections are not available to them in those statuses. This distinction is operationally significant because state active-duty and Title 32 forces, if allowed by state law, can provide support to federal, state, local, and tribal law enforcement agencies and respond to domestic sUAS threats or incidents under state authority. National Guard personnel responding to a domestic sUAS threat pursuant to Title 10, USC (§130i), authorities are required to be in a Title 10 duty status while conducting C-sUAS activities. The joint force requires specific authorization under Title 10, USC (§130i), or other applicable federal authority, to conduct C-sUAS operations in the United States or its territories. All National Guard C-sUAS operations have been approved through the standard DoW procedures for countering UA.

(3) The Department of Homeland Security, Department of Justice, and Department of Energy, along with delegated component agencies, possess independent statutory authorities to counter sUAS threats to their respective facilities and missions. Personnel may detect, identify, and track UASs; warn operators; disrupt UASs; and seize or destroy sUAS that pose a credible threat. Protection applies specifically to designated federally covered facilities or assets, which include high-risk critical infrastructures, federal facilities, or assets. The statutory authority of Title 6, USC (§124n), and Title 10, USC (§6227), allow these agencies to take actions that might otherwise violate Title 18, USC (wiretap/pen-trap, computer fraud, aircraft sabotage); Title 49, USC (aircraft piracy); or other laws. Homeland C-sUASs require coordination across departments and with the FAA, which retains authority over the National Airspace System.

(4) Counter-sUAS operations within CONUS often require the use of RF jamming, which is an EMS operations activity. Title 47, USC, directs authority within the United States and its possessions to regulate federal and civil use of the managed portion of the radio spectrum through the Department of Commerce. There are two primary

jamming authorities controlled (but delegated) by the Department of Commerce's National Telecommunications and Information Agency. One authority supports tests, training, and exercises through DoW as the lead federal agency. The other authority is coordinated through the Department of Justice in support of homeland security missions. See the National Telecommunications and Information Administration *Manual of Regulations and Procedures for Federal Radio Spectrum Management;* Chairman of the Joint Chiefs of Staff Manual 3212.02, *(U) Performing Electromagnetic Attack in the United States and Canada for Tests, Training, and Exercises;* and CJCSM 3212.03, *Performing Tests, Training, and Exercises Impacting the Global Positioning System.*

b. **During Overseas Operations**

(1) C-sUAS operations outside the United States are governed by CCMD authorities derived from Title 10, USC; the *Unified Command Plan;* and theater-specific ROE approved by SecWar. Combatant commanders (CCDRs) possess the authority to direct C-sUAS operations within their AORs in accordance with their operational plans, execute orders, and standing ROE per Chairman of the Joint Chiefs of Staff Instruction 3121.01, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

(2) SOFAs, HN laws, and bilateral security agreements may impose additional restraints on C-sUAS operations in specific countries. Commanders ensure C-sUAS ROE/rules for the use of force are coordinated with HN authorities where applicable and that engagement criteria account for the presence of civilian aircraft operating in the same airspace.

2. Responsibilities

a. **CCMDs.** CCDRs and their staffs are responsible for integrating C-sUAS capabilities into operational and contingency plans within their AORs. This includes assessing the theater-specific sUAS threat, identifying C-sUAS capability requirements, establishing theater ROE and rules for the use of force for C-sUAS operations, and prioritizing the allocation of C-sUAS assets. CCDRs with AORs should develop theater C-sUAS architectures that integrate detection, tracking, identification, and defeat capabilities into existing AD and force protection frameworks. All other CCDRs address C-sUAS requirements within their respective functional areas based on assessed threats.

b. **Joint Interagency Task Force 401 (JIATF 401).** JIATF 401, established through a SecWar memorandum and reports to the Deputy Secretary of War, aligns authorities and resources to rapidly deliver Joint C-sUAS capabilities to joint warfighters, defeat enemy threats, and promote control over national airspace. JIATF 401 is an independent Chairman of the Joint Chiefs of Staff-controlled activity.

c. **Services.** The Military Departments are responsible, under Title 10, USC, for organizing, training, and equipping forces with C-sUAS capabilities to meet CCDR requirements. The Services must comply with DoW issuances covering acquisition and EMS guidelines for all spectrum-dependent systems, including COTS systems. The Services develop Service-specific TTP for C-sUAS employment within their formations. The Services establish programs of instruction, qualification standards, and training programs that prepare individuals and units to operate, maintain, and integrate C-sUAS

systems. The Services resource C-sUAS materiel programs through their respective programming and budgeting processes to align C-sUAS training standards and capability to operational formations.

d. **Service Components—Outside the Continental United States (OCONUS) Operations**

(1) Service components retain responsibility for C-sUAS operations at enduring OCONUS installations under force protection authorities per Title 10, USC. Installation commanders execute C-sUAS operations to protect assigned forces, facilities, and assets.

(2) Service component C-sUAS responsibilities for enduring OCONUS installations include:

(a) Providing organic C-sUAS capabilities appropriate to installation threat level, defended asset criticality, and theater priority as established by the CCDR.

(b) Establishing installation C-sUAS standard operating procedures consistent with theater ROE, rules for the use of force, HN legal authorities, and SOFA provisions.

(c) Integrating installation C-sUAS sensors into theater air surveillance networks and COP architecture through theater-standard data links and formats.

(d) Submitting installation C-sUAS airspace coordination measures (ACMs) through HN and theater airspace control order (ACO)/air tasking order (ATO) cycles for planned operations and maintaining coordination procedures with the theater air operations center for dynamic activations.

(e) Coordinating installation C-sUAS EW employment with the HN and theater JEMSOC [joint electromagnetic spectrum operations cell] to prevent electromagnetic interference (EMI) with theater operations.

(3) The HN and theater area air defense commander (AADC):

(a) Provides oversight and coordination for OCONUS installation C-sUAS operations.

(b) Establishes theater C-sUAS ROE and engagement authorities applicable to all Service component force protection operations within the theater.

(c) Integrates installation C-sUAS sensors into theater air surveillance architecture and COP.

(d) Deconflicts installation C-sUAS engagement zones with theater integrated air and missile defense (IAMD) systems, adjacent installation C-sUAS operations, and theater air operations.

(e) Provides theater-level sUAS threat intelligence, enemy tactics and techniques updates, and C-sUAS lessons learned to installation commanders.

(f) Coordinates theater C-sUAS capability augmentation to installations during elevated threat periods or when sUAS threats exceed installation organic C-sUAS capabilities.

(4) CCDR responsibilities for non-contingency OCONUS C-sUAS operations include establishing theater policy for:

(a) HN coordination requirements and SOFA implementation guidance for C-sUAS operations, including engagement authorities over HN sovereign territory and coordination with HN AD forces.

(b) Integration with multinational AMD architecture where applicable, including data-sharing protocols with allied AD systems and combined engagement coordination procedures.

(c) Prioritization criteria for allocation of theater C-sUAS capabilities across installations based on threat assessment, asset criticality, and operational requirements.

(d) Coordination between installation force protection C-sUAS operations and theater AD operations to ensure unity of effort across the theater.

e. **Interagency.** C-sUAS operations, particularly in the homeland, require coordination across DoW and multiple federal departments and agencies. The Department of Homeland Security, through the United States Customs and Border Protection Agency, the United States Secret Service, and the Cybersecurity and Infrastructure Security Agency, possesses both authorities and capabilities for C-sUASs within their respective mission area. The Department of Justice, through the FBI, possesses law enforcement authorities relevant to sUAS threats involving criminal activity or domestic terrorism. The Department of Energy possesses C-sUAS authorities for the protection of certain special nuclear material-related facilities and national laboratories. Counter-sUAS activity that may affect civil aviation requires coordination with the FAA. Departments with statutory C-sUAS authority are also required to coordinate with the Department of Transportation regarding the implementation of their respective authorities. Interagency coordination is formalized through memoranda of agreement, joint operating procedures, and interagency working groups. JIATF 401 serves as the DoW focal point for interagency C-sUAS coordination, integrating across more than 50 federal agencies with equities in the C-sUAS mission. A best practice technique for National Guard forces serving in support of a lead federal agency (i.e., Department of Homeland Security, Department of Justice, FBI) C-sUAS mission is to deputize those National Guard forces for the duration of the mission.

(1) Detailing the National Guard forces to the lead federal agency is also an option, but the deputization of the National Guard forces provides a larger legal safety net of authorities for the Guard members, the National Guard institution, and the lead federal agency.

3. Establishing Command and Control and the Networks for Counter Small Unmanned Aircraft System Operations: Combatant Command to the Tactical Edge

C-sUAS requires a C2 architecture that enables CCMD-level situational awareness (SA) to tactical-level engagement authority. The sUAS threat can significantly compress engagement timelines to seconds, which may require pre-delegated authorities, automated sensor-to-shooter linkages, and distributed decision making at the lowest practical echelon.

a. CCDRs establish C-sUAS C2 frameworks that integrate existing AD and fire control networks. This includes integration with C2 architectures, AMD systems, and tactical data links that enable track sharing across echelons. The EMS is both an enabler and a contested environment for C-sUAS C2. EW systems used for C-sUAS engagement operate in the same spectrum as friendly communications and navigation systems, requiring deliberate spectrum management and deconfliction at every echelon. However, fiber-optic, sUASs are prolific and not affected by most EW systems.

b. AI capabilities may be integrated into C-sUAS C2 to accelerate detection, classification, and engagement. AI-enabled systems process sensor data, identify threat patterns across multiple sensors, and recommend optimal engagement solutions, faster than human operators. However, engagement decisions remain a command responsibility, and the integration of AI into C-sUAS C2 is governed by established ROE, rules for the use of force, and the law of armed conflict.

c. A C-sUAS network is fundamental to maintaining protection in the current operational environment and requires a network infrastructure that facilitates operations at a speed and scale that enables SA, provides commanders with tactical flexibility, and enables a cost-efficient defense against a wide array of aerial threats. This network should be tightly linked to the base/area warning (e.g., GIANT VOICE) network to expedite personnel response to the incoming threat (e.g., displacement to bunkers; movement of equipment away from predictable, targetable locations).

(1) A C-sUAS network should satisfy several key requirements. It must be capable of supporting a comprehensive and real-time COP, enabling data fusion and the integration of disparate sensors. Furthermore, the network should be integrated into the C2 structure and feature interoperable and standardized interfaces, while being layered, redundant, and secure against cyberspace and other threats. Figure below graphically displays a sample C-sUAS COP.

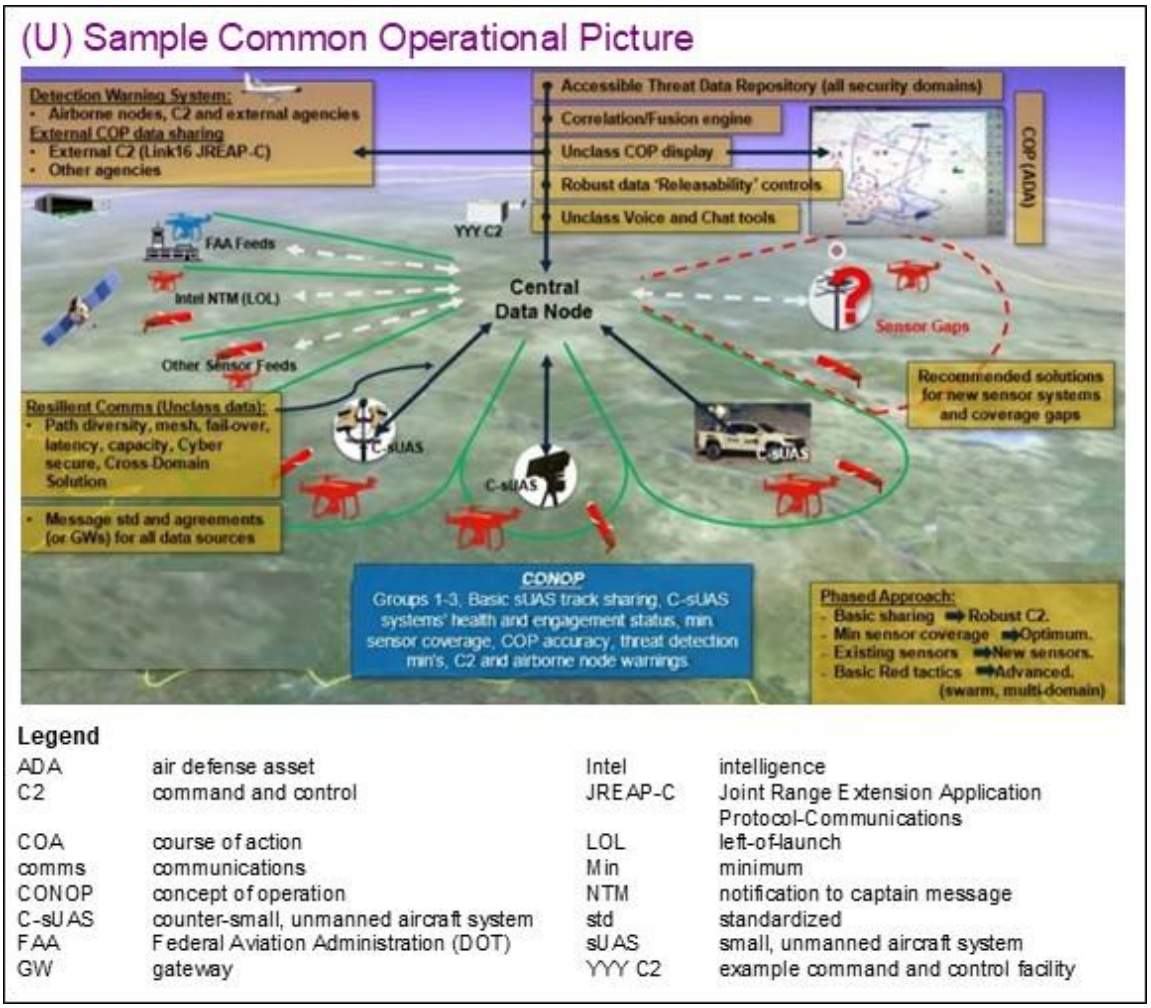


Figure. Sample Common Operational Picture

(2) A critical capability for any C-sUAS C2 network is the ability to generate, support, and disseminate a real-time COP. The data from a multitude of sensors is integrated to create a COP that provides commanders and operators with high-fidelity SA necessary to make timely and informed decisions. A shared and accurate COP is the foundation upon which C-sUAS airspace management and engagement operations are built.

(3) To produce a real-time and accurate COP, the network infrastructure must integrate and fuse data from a variety of sensors. The employment of a modular and open architecture is an essential attribute, as it allows for the rapid integration of new sensor technologies as they are procured and fielded by joint and multinational forces. This integration ensures the C-sUAS network can adapt to emerging threats and incorporate the most effective sensor solutions available, regardless of manufacturer or origin.

(4) To support a layered defense-in-depth, the C-sUAS C2 network should be interoperable among all participating systems. To communicate and share data across the joint force and with multinational partners, the network must be provisioned to support

standardized data interfaces and plug-and-play capabilities. This is achieved through the development, publication, and enforcement of a data standardization plan that is made readily available to all C-sUAS providers, enabling seamless integration and the ability to present threats with multiple, complementary defensive capabilities.

(5) Beyond the external capabilities it enables, the C-sUAS network requires a redundant, resilient, and secure communications network engineered with sufficient bandwidth and reliability to support the real-time data flows required by advanced C-sUAS sensors and shooters. Cyberspace security is a paramount concern. The network and all its constituent components require protection from enemy cyberspace attacks that could disrupt, degrade, or disable C-sUAS capabilities at a critical moment.

(6) A C-sUAS network should be built on a foundation that supports a COP, ensures interoperability, and enables a layered defense. It requires a modular architecture to allow for the rapid integration of emerging technologies while simultaneously being resilient against enemy cyberspace attacks and electromagnetic attacks (EAs). Only through the development of such a network can the joint force be prepared to meet the evolving threat of UASs.

CHAPTER IV
PLANNING

1. Integration with the Joint Planning Process

a. C-sUAS operations should be integrated into the joint planning process. The Russia-Ukraine conflict demonstrated that C-sUAS operations cannot be treated as an ancillary capability; it is a requirement that impacts force survivability, operational tempo, and mission success.

b. During mission analysis, planners assess the sUAS threat as one factor shaping courses of action (COAs). Russian forces demonstrated employment of OWA UASs layered with ballistic and cruise missiles specifically to overwhelm Ukrainian AD. This layering approach forced defenders to make resource allocation decisions and created windows of vulnerability that the enemy could exploit for follow-on strikes.

c. **EMS Access Analysis.** Identify EMS requirements and conduct analysis to ensure unrestricted access to EMS resources that may prevent integration efforts. Operation EPIC FURY's experience shows that the lack of pre-coordination exponentially increased EMI incidents.

d. C-sUAS planning considerations should be embedded in each joint planning process step.

(1) **Mission Analysis.** Identify critical assets requiring C-sUASs protection, assess enemy sUAS capabilities and employment patterns, and determine C-sUAS force requirements. Include enemy sUAS capabilities in risk-to-mission and operational risk analysis.

(2) **COA Development.** Integrate C-sUAS capabilities into each COA, ensuring layered defense approaches rather than reliance on single solutions. Ukraine's experience shows that no static countermeasures work; the enemy may adapt within 2-to-4-week cycles, requiring continuous evolution of defensive approaches.

(3) **COA Analysis and Wargaming.** Use red team sUAS employment against friendly COAs, to identify vulnerabilities in C2 nodes, logistics hubs, and maneuver forces. Wargame enemy adaptation to friendly C-sUAS measures.

(4) **COA Comparison.** COAs should be compared against criteria that are based on optimal protection against enemy UASs while still providing flexibility for friendly forces to achieve mission objectives.

(5) **Orders Development.** Clearly articulate C-sUAS responsibilities, engagement authorities, ACMs, and integration with fires and AD systems.

e. C-sUAS planning requires understanding that this is fundamentally a planning problem, not merely a technical one. As observed by advisors supporting Ukrainian forces, terrain changes, partner capabilities, and enemy capabilities.

2. Joint Intelligence Preparation of the Operational Environment

a. **Small UAS-Specific JIPOE [Joint Intelligence Preparation of the Operational Environment].** Traditional JIPOE processes require modification to address the unique characteristics of sUAS threats. Unlike conventional air threats, sUASs can operate from virtually anywhere, employ diverse control methods, and adapt rapidly to countermeasures.

b. Small UAS-specific JIPOE should address:

(1) **Terrain Analysis.** Identify likely sUAS launch sites, approach corridors, micro-terrain masking, the clutter environment (e.g., urban RF noise and thermal crossover periods), and dead zones. Small UASs can exploit terrain masking that larger aircraft cannot, requiring detailed analysis of micro-terrain features.

(2) **Weather Effects.** Assess how weather impacts both threat sUAS operations and friendly C-sUAS sensors and effectors. Wind, precipitation, and visibility affect sUAS differently than conventional aircraft.

(3) **Infrastructure Analysis.** Map cellular tower locations, coverage footprints, carrier frequencies, fiber-optic networks, and other infrastructure that adversaries may exploit for sUAS C2. Russian forces demonstrated integration of Ukrainian cellular networks into Shahed sUAS operations.

(4) **Enemy Force Analysis.** Understanding enemy sUAS unit identification, organization, equipment holdings, doctrine/TTP, and training proficiency. Russia is establishing separate unmanned systems forces, changing how sUAS capabilities are organized and employed.

c. **Enemy Adaptation Tracking.** The most critical JIPOE function for C-sUAS operations is continuous tracking of enemy adaptation. Intelligence organizations should establish processes to:

(1) Monitor enemy sUAS modifications (e.g., new jamming-resistant antennas, different warheads, alternative control methods).

(2) Track changes in employment tactics (e.g., route planning, saturation techniques, decoy integration).

(3) Assess effectiveness of friendly C-sUAS measures and identify enemy counter-adaptations.

(4) Disseminate enemy updates to units as quickly as possible. Increase coordination and synchronization with the intelligence community to gain timely intelligence reports and products to support organizations' mission. Successful models from Ukraine show intelligence cells embedded with C-sUAS units, providing real-time analysis and immediate feedback loops.

(5) Establish an intelligence collection plan based on an effective and flexible collection strategy, informed by operational priorities, to answer the commander's critical

information requirements and priority intelligence requirements.

d. **Pattern Analysis and Predictive Intelligence**

(a) Enemies develop patterns in s UAS employment that enable predictive analysis.

(b) **Targeting.** When conducting long-range strikes, Russian forces have shown the ability to prioritize their targets. However, they often struggle to achieve accurate results with their precision-guided weapons, highlighting a shortfall in their target acquisition capabilities. Understanding these patterns enables defensive resource allocation.

(c) **Route Analysis.** OWA sUAS route planning reveals enemy intent to distract and disrupt AD systems while penetrating deeper into defended airspace. Analyzing historical routes enables prediction of future approach corridors.

(d) **Saturation Techniques.** Pattern analysis of swarm sizes, timing, and target sets enables prediction of major attack preparations, providing warning for defensive preparations. Analysis of enemy saturation techniques can also reveal how the enemy layers UASs with other forms of attack such as BMs and EW jamming.

(e) Intelligence organizations should leverage AI tools to process the volume of sUAS-related data and identify patterns human analysts might miss. However, human analysis remains essential for understanding enemy intent and operational context.

3. Force Protection Planning

a. **Defended Asset List and Critical Asset List.** C-sUAS force protection begins with disciplined asset prioritization. The reality of limited C-sUAS resources against proliferated threats demands difficult choices about what to defend and at what level and acceptance/expectation of casualties and modification of response actions (e.g., congregating in a bunker, which is the conditioned response to a theater battle management threat/air attack, may be undesirable if a sUAS can be guided through the opening to the bunker and detonate inside it).

b. Defended asset list/critical asset list development for C-sUAS considers:

(1) **Asset Criticality.** Not all assets warrant the same level of C-sUAS protection. Nuclear sites, C2 nodes, logistics hubs, and AD systems typically require priority protection.

(2) **Vulnerability.** Some assets are inherently more vulnerable to sUAS attack (e.g., fuel storage, ammunition depots, aircraft on the ground) and may require enhanced protection despite lower operational criticality.

(3) **Consequence of Loss.** Assess tactical, operational, and strategic effects of asset loss. Loss of a single C2 node may have cascading effects across the OA.

(4) **Defendability.** Some forces may be too dispersed or mobile to defend with

available C-sUAS resources. Planners should make realistic assessments of what the force can protect.

(5) Ukraine's experience shows that UAS threats excel at disruption, forcing dispersal, triggering AD expenditure, and imposing repair and protection costs, even when they cannot achieve outright destruction. This reality should inform critical asset list/defended asset list prioritization; protecting operational tempo may be as important as protecting specific assets. Similarly, this may affect air asset allocation. That is, a greater number of defensive counter air missions may be required of the combined force air component commander that pulls away from the ability to interdict or conduct offensive counter air.

Refer to Joint Publication (JP) 3-01, Countering Air and Missile Threats, *for more details on critical asset list and defended asset list development.*

c. Fixed installations present both advantages and challenges for C-sUAS operations. Advantages include the ability to establish sensor networks, pre-position C-sUAS capabilities, and develop defense plans. Challenges include predictable locations that enable enemy planning and the requirement to defend large perimeters with finite resources.

d. Integration of C-sUAS into base defense requires:

(1) **Layered Detection.** Establish multiple sensor rings using complementary technologies (e.g., radar, EO-IR, acoustic, and RF). Ukrainian forces have demonstrated effective integration of passive sensors into MANETs, creating resilient detection architectures. Sensor placement should account for terrain masking, mutual support (overlapping coverage), and redundancy.

(2) **Engagement Zones.** Define clear zones for different engagement authorities and shooter types. Outer zones may permit engagement with kinetic fires, while engagements within inner zones involve considering the full range of kinetic and non-kinetic fires solutions due to the proximity to high-value assets and personnel.

(3) **Integration with Physical Security.** C-sUASs cannot operate in isolation from traditional base defense. Coordinate with ground security forces to address UASs that penetrate defenses or conduct forced landings. Consider dispersing or frequently moving key assets (e.g., do not park an E-3 AWACS [Airborne Warning and Control System] on the same spot. Move it from place to place around the ramp or on the parallel or other taxiways).

(4) **Airspace Coordination.** Establish airspace control measures, such as restricted operating zones (ROZs), that enable simultaneous, friendly air operations and C-sUAS engagements. This is particularly challenging within the United States, its territories, and possessions, where FAA coordination is required.

For operations within the United States, its territories, and possessions, JP 3-27, Homeland Defense, *provides the framework, with additional considerations for domestic legal authorities and coordination with civil authorities. For overseas operations, JP 3-*

10, Joint Security Operations in Theater, *applies, with greater operational flexibility but increased threat complexity.*

e. **Maneuver Force Protection.** Protecting maneuver forces has different challenges than fixed-site defense. Maneuver units maintain mobility while defending against sUAS threats that can detect, track, and engage them throughout the depth of operations. Key considerations include:

(1) **Mobile C-sUAS.** Maneuver forces require C-sUAS capabilities that move with them. This typically means vehicle-mounted systems with rapid emplacement/displacement capability.

(2) **Distributed Operations.** Maneuver forces disperse to reduce vulnerability, requiring C-sUAS coverage across distributed formations without creating gaps adversaries can exploit.

(3) **Sensor-to-Shooter Integration.** Maneuver forces must integrate C-sUAS capabilities with C2 to maintain a COP and enable engagement coordination within rapid timelines. Successful integration of detection systems directly into fire control networks enables immediate engagement.

(4) **Passive Defense.** Maneuver forces employ camouflage, concealment, deception, and dispersion to reduce sUAS detection and targeting effectiveness. Active C-sUAS measures complement but cannot replace passive defense.

(5) **Electromagnetic Signature Management.** UASs increasingly employ EW and SIGINT for detection and targeting. To survive, the joint force manages electromagnetic emissions to minimize EMI incidents while maintaining necessary communications.

f. **Maritime Force Protection.** Maritime forces face unique C-sUAS challenges. Ships present large, high-value targets that are difficult to conceal. The maritime environment affects sensor performance and limits engagement options. At the tactical level, the AMD commander is the warfare commander responsible for developing the maritime force's AMD plan that incorporates operational-level guidance. This includes the maritime force's C-sUAS protection. Maritime C-sUAS considerations include:

(1) **Layered Defense.** The AMD commander normally employs a defense-in-depth approach when assigning forces for C-sUAS protection. Ships employ multiple C-sUAS layers, including long-range detection, medium-range soft-kill (e.g., EW), and close-range hard-kill (e.g., kinetic/DE). The time and distance challenges of distributed maritime forces require establishing appropriate kill webs in maritime C-sUAS operations, which, in some cases, pairs targets and weapons for clear and rapid engagement. Early planning, establishing and rehearsing kill webs, and rehearsing C-sUAS employment is vital. The AMD commander should know what specific weapon systems or capabilities are available to incorporate them into mission planning and stationing. Planning aims to ensure proper division of airspace amongst shooters and establishing hand-off ranges between the different systems.

(2) **Integration with Ship Self-Defense.** C-sUASs integrate with existing ship self-defense systems (e.g., guns, ESSM [Evolved Sea Sparrow Missile]) to provide layered protection against air and missile threats.

(3) **Port and Anchorage Defense.** Ships in port or at anchor are particularly vulnerable (ship sensors have limited coverage aft and abeam when moored; ship weapons have restricted firing arcs near port infrastructure); land-based C-sUAS augmentation is required which further requires joint land-maritime C-sUAS integration.

(4) **Environmental Considerations.** Maritime environment affects radar performance (e.g., sea clutter), electro-optical systems (e.g., salt spray, fog), and acoustic sensors (e.g., wind, wave noise). Plan for degraded sensor performance.

(5) **Integration of Embarked Land Force Capabilities.** For amphibious warfare ships and other ships in which the landing forces have embarked, the landing force C-sUAS capabilities should be included in integration planning.

g. **C2 Node Defense and Protection.** C2 nodes are often high-priority targets for the enemy. Loss of C2 can have cascading effects across the force. Protection priorities include:

(1) **Hardening.** Where possible, locate C2 nodes in hardened facilities that can withstand sUAS payloads.

(2) **Redundancy.** Establish redundant C2 capabilities so loss of a single node does not create operational paralysis.

(3) **Mobility.** Mobile C2 nodes are harder to target but require C-sUASs that move with them.

(4) **Electromagnetic Deception.** C2 nodes emit significant electromagnetic signatures. Employ emission control, decoys, and deception to complicate enemy targeting.

(5) **Priority Defense.** Allocate premium C-sUAS capabilities to C2 node defense, including multiple sensor types and engagement options.

h. **Logistics Node Defense and Protection.** Logistics nodes (e.g., supply points, maintenance facilities, fuel storage, ammunition depots) are lucrative sUAS targets. They are often predictable in location and contain flammable or explosive materials, and their loss directly impacts operational tempo. Logistics C-sUAS protection requires:

(1) **Dispersion.** Avoid concentrating logistics in single locations. Dispersed logistics may be harder to target, yet they still require C-sUAS coverage.

(2) **Hardening and Separation.** Use revetments, berms, and separation distances to limit damage from successful sUAS strikes.

(3) **Rapid Reconstitution.** Plan for logistics node reconstitution after sUAS strikes. Pre-position materials and equipment for rapid repair.

(4) **Deception.** Employ decoy logistics sites to complicate enemy targeting and

waste their sUAS resources.

(5) **Integration with Convoy Operations.** Logistics convoys are vulnerable to sUAS attack. Integrate mobile C-sUAS capabilities into convoy security operations.

i. **Dispersed and Expeditionary Force Protection**

(1) **Rotational and Temporary Force Locations.** Forces operating from rotational or temporary locations require:

(a) Mobile C-sUASs that deploy with the force.

(b) Mobile C-sUAS capability organic to deploying units rather than reliance on fixed-site systems.

(c) Prioritization criteria for dispersed sites based on asset criticality, vulnerability, consequence of loss, and ability to defend.

(d) Interim C-sUAS coverage for temporary high-value targets (e.g., construction sites, logistics nodes, infrastructure projects) until permanent systems are installed.

(2) **Multinational Force Integration.** US forces operating as part of multinational formations require:

(a) C-sUAS integration with HN and allied forces.

(b) Common ROE across contributing nations (typically more restrictive than US unilateral ROE).

(c) Interoperable C2 systems enabling track-sharing between US, HN, and other contributing nation C-sUAS sensors.

(d) Coordinated engagement zones preventing friendly fire between US and allied C-sUAS effectors.

(e) Integration with HN territorial defense plans and AD command structures.

(3) **HN Base Defense Integration**

(a) Legal authorities for C-sUAS operations on HN installations are governed by SOFAs.

1. SOFAs typically provide US forces authority to conduct C-sUAS operations for protection of US forces and assets but require HN notification and coordination.

2. Engagement of UASs over HN sovereign territory (outside US installation boundaries) typically requires HN approval, except in cases of imminent threat to US forces (self-defense provisions in SOFAs).

3. C-sUAS EW employment must comply with HN spectrum regulations and coordinate through HN spectrum management authorities.

(b) Integration with HN base defense forces requires coordination with HN

military police, territorial defense forces, or facility protection units responsible for installation outer perimeter security.

(c) Shared installations require unified C-sUAS architecture with clear US/HN responsibility delineation.

1. US forces typically provide C-sUAS sensors and C2 architecture.

2. HN forces provide outer-layer security and ground-based response to landed/crashed UASs.

3. Engagement authority is pre-coordinated through installation defense plans, with US forces authorized to engage threats to US assets and HN forces authorized to engage threats to national assets.

j. **Force Protection and Base Defense Execution**

(1) **Installation Commander C-sUAS Authorities.** Installation commanders execute C-sUAS operations under force protection authorities to defend assigned forces, facilities, and assets against sUAS threats.

(a) Installation commanders are delegated engagement authority for sUAS threats to installation forces and assets consistent with theater ROE, applicable rules for the use of force, and self-defense provisions under international law and SOFA agreements.

(b) C-sUAS execution is integrated into installation defense plans per JP 3-10, *Joint Security Operations in Theater,* antiterrorism plans and force protection programs as a critical capability for countering sUAS threats to installation operations, personnel, and mission-critical assets.

(c) Installation commanders establish C-sUAS standard operating procedures addressing detection and identification; tracking and classification; engagement decision-making processes; effector employment coordination; and post-engagement actions, including battle damage assessment and sUAS exploitation.

(2) **Base Defense Operations Center (BDOC) Battle Management.** The BDOC executes C-sUAS operations for installation defense as the tactical C-sUAS battle management element. The BDOC:

(a) Maintains C-sUAS COP integrating organic sensor feeds, theater air surveillance track data received via tactical data links, and HN AD tracks where coordination agreements exist.

(b) Coordinates dynamic C-sUAS airspace activations with the theater air operations center through established liaison procedures and communications architecture, ensuring deconfliction with theater air operations, adjacent installation C-sUAS operations, and HN airspace users.

(c) Executes engagement decisions consistent with installation

commander's pre-delegated authorities, theater ROE, and established engagement decision matrices.

(d) Coordinates with installation emergency services for response to landed or crashed UASs, including security forces for site security, explosive ordnance disposal (EOD) for render-safe procedures, and intelligence personnel for technical exploitation.

(e) Maintains communications with the theater air operations center, adjacent installation BDOCs, and HN AD coordination centers to enable coordinated response to sUAS threats transiting multiple AORs.

(3) **Pre-Delegated Engagement Authorities.** Time-sensitive sUAS threats require pre-delegated engagement authorities to enable responsive defensive action within compressed engagement timelines.

(a) Installation commanders establish engagement decision matrices based on sUAS flight profile characteristics, proximity to critical assets, threat indicators from intelligence preparation, and consequence of engagement versus non-engagement, enabling BDOC battle management personnel to execute engagements without commander approval for specified threat conditions.

(b) Pre-delegated authorities should address the following threat categories:

1. Immediate threats to aircraft operations. UASs within approach/departure corridors during active flight operations, UASs at altitudes conflicting with published instrument procedures, or UASs exhibiting flight profiles indicating intent to collide with aircraft.

2. UASs penetrating established restricted areas around ammunition storage areas, fuel storage facilities, mission-critical C2 nodes, or other assets designated in installation defense plans as requiring immediate defense.

3. UASs exhibiting hostile intent indicators, including multiple passes over facilities, indicating reconnaissance for attack; coordinated multi-sUAS approaches, suggesting massed attack; flight profiles consistent with observed enemy attack patterns; or UASs maneuvering to avoid detection, suggesting enemy intent.

(c) All engagements executed under pre-delegated authorities require immediate notification to the installation commander and theater air operations center, with a formal engagement report submitted within timelines established by theater policy.

(d) Installation commanders should establish engagement decision aids (e.g., decision matrices, automated decision support tools) that enable BDOC personnel to rapidly assess threat conditions against pre-delegated authority criteria during high-tempo operations.

(4) **Integration with Theater AD Architecture.** Installation C-sUAS operations integrate with theater AMD while maintaining force protection execution authorities.

(a) Installation C-sUAS engagement zones are coordinated with theater

AADC and published in theater ACOs as short-range air defense engagement zones (SHORADEZs) or weapons free zones as appropriate to installation defense requirements.

(b) Installation C-sUAS sensors provide track data to theater COP via Link 16 or theater-standard tactical data links, enabling theater air operations center SA of installation C-sUAS operations.

(c) The theater air operations center provides cueing to the installation BDOC for sUAS tracks detected by theater air surveillance sensors approaching installation areas, enabling extended warning time for installation defense preparations.

(d) Installation commanders coordinate with the theater AADC for augmentation of installation C-sUAS capabilities during elevated threat periods, major exercises, or when sUAS threats exceed installation organic C-sUAS capacity, with augmentation forces operating under tactical control of the installation commander for force protection mission.

4. Integration with Joint Fires and Air Defense

a. **AMD Integration.** C-sUAS operations must integrate seamlessly with AMD to provide comprehensive defense against the full range of air and missile threats. Russian employment of layered attacks, combining OWA UASs, BMs, and cruise missiles, specifically target seams between C-sUAS and traditional AMD systems. Integration requirements include:

(1) **COP.** C-sUAS sensors should feed into the AMD COP, providing commanders comprehensive air threat awareness. Ukrainian forces demonstrated effective integration of radar and optical sensor data with automatic sharing across adjacent units regardless of parent organization. Additionally, AMD sensors should feed into the C-sUAS COP.

(2) **Engagement Coordination.** Establish clear engagement priorities and coordination procedures between C-sUAS and AMD systems. Commanders should consider requesting a joint engagement zone (JEZ) as part of a comprehensive, layered AMD. Avoid fratricide while ensuring no gaps in coverage.

(3) **Resource Management.** Coordinate employment of systems that can engage both traditional air threats and UASs (e.g., Patriot, NASAMS [Norwegian Advanced Surface-to-Air Missile System]) to optimize resource allocation.

(4) **Decentralized Execution.** Lower echelons require authority and capability to engage sUAS threats without waiting for higher headquarters approval. Ukrainian experience shows the importance of pushing display only Link 16 pictures to lower echelons to increase SA and enable decentralized engagement.

b. **Counterair Operations Coordination.** C-sUAS operations coordinate with offensive counterair (OCA) and defensive counterair (DCA) operations. This includes:

(1) **OCA.** Coordinate C-sUAS intelligence on enemy's larger UAS launch

sites, production facilities, and C2 with OCA targeting. Prior-to-launch strikes against UAS infrastructure reduce defensive burden.

(2) **DCA.** Integrate large C-sUAS into DCA planning, ensuring comprehensive defense against air threats. Establish clear responsibilities between fighter aircraft, SAMs [surface-to-air missiles], and other C-sUAS capabilities.

(3) **Airspace Control.** Coordinate C-sUAS engagement zones with airspace control measures to enable simultaneous friendly air operations and C-sUAS engagements.

(4) **Fighter Integration.** Fighters can engage some sUAS threats, particularly larger, faster systems. Fighters also bring sensor capabilities and may be utilized in that manner as part of the integrated kill web in addition to their engagement capabilities. Coordinate fighter employment against UASs with ground-based C-sUASs to optimize resource allocation.

c. **All-Domain Fires Integration.** C-sUAS operations increasingly require integration across all domains.

(1) **Sensor Integration.** Fuse data from air, ground, maritime, space, and cyberspace sensors to provide a sUAS threat picture. Using a combination of sensors (e.g., radar, EO-IR, acoustic, RF) is essential for detecting enemy UASs.

(2) **Weapons Coordination.** Coordinate employment of kinetic and non-kinetic weapons across domains. Effects in cyberspace and the EMS may enable kinetic fires engagement or produce standalone effects.

(3) **Cross-Domain Targeting.** Larger enemy UASs may depend on multi-domain networks (e.g., space-based navigation, terrestrial communications, C2 in cyberspace). Target these networks across domains to degrade sUAS effectiveness.

(4) **Joint Fires Coordination.** Integrate C-sUAS targeting into joint fires processes, ensuring sUAS launch sites and support infrastructure are targeted as appropriate.

d. **EMS Management**. EMS deconfliction of C-sUAS radar and C2 systems is required across all mission partners to ensure effective operations. This requires coordination for frequency assignments prior to employment.

5. Joint Logistics Planning and Integration in Counter-Unmanned Aircraft System Operations

a. **Logistics Vulnerability in Contested Environments**. Joint logistics nodes present high-value, predictable targets for enemy UASs due to their concentration of personnel, equipment, materiel, and electromagnetic signatures from communications and material handling equipment and relatively static locations. CCDRs need to integrate joint logistics planners into C-sUAS planning to prioritize protection of critical sustainment operations.

b. **C-sUAS Planning Integration**. Joint logistics planners need to accomplish the following as part of planning:

(1) Identify critical logistics nodes and movement schedules requiring C-sUAS protection priority based on operational phasing and sustainment criticality.

(2) Coordinate logistics activities with C-sUAS sensor coverage and engagement zones to ensure protection during high-signature operations (e.g., aircraft downloads, bulk fuel transfers, convoy staging).

(3) Develop contingency sustainment plans for operations under degraded or denied C-sUAS conditions.

c. **Adaptive Logistics Operations Under Small UAS Threat**. To reduce sUAS targeting effectiveness while maintaining sustainment, logistics operations JFCs can consider:

(1) Dispersed logistics posture with small, mobile nodes that complicate enemy sUAS targeting.

(2) Temporal dispersion of high-signature activities to periods of enhanced C-sUAS coverage or reduced threat windows.

(3) Rapid displacement of mobile logistics nodes following resupply operations.

(4) Redundant supply routes and methods to maintain sustainment if primary nodes are compromised by sUAS attack.

d. **Sustainment and Supply Chain Management for C-sUAS Systems**

(1) C-sUAS operations require a comprehensive approach to sustainment and supply chain management. As sUAS threats evolve rapidly and proliferate across OAs, the joint force requires timely procurement, maintenance, and replenishment of C-sUAS capabilities and components. Robust logistics and resilient supply chains are essential to maintaining operational readiness, minimizing system downtime, and enabling agile responses to emerging threats in both expeditionary and homeland defense contexts.

(2) Specific areas of consideration include the following:

(a) Sensors, effectors, and software updates, to maintain operational effectiveness against evolving sUAS threats.

(b) Resilient supply chains for C-sUAS operations, prioritizing redundancy and mitigation strategies for potential disruptions caused by enemy actions, cyberspace threats, or commercial-market volatility.

(c) Integrating maintenance, repair, and lifecycle support planning for C-sUAS operations into joint logistics operations; enabling sustained readiness; and minimizing downtime in both expeditionary and homeland defense contexts.

(d) Coordinating with Service, interagency, and commercial partners to leverage shared logistics networks and accelerate fielding of emerging C-sUAS technologies and capabilities.

6. Joint Force Interoperability Challenges

JFCs and staff face interoperability challenges in every operation, and the C-sUAS fight is no different. While not unique individually, recent combat operations involving the planning and execution of C-sUAS operations include the following technical, procedural and cross-domain challenges, as well as the existing joint fires coordination challenge:

a. **Technical Interoperability Challenges**

(1) **C2 Integration**

(a) **Sensor Fusion Across Services and Partners.** C-sUAS networks need to integrate disparate sensors from multiple vendors, services, and nations into a unified COP.

(b) **Data Standardization.** Multinational operations require fusion of US, allied, and HN sensor data using different formats. Track quality metadata must be preserved across fusion nodes and include common track numbering across US and allied systems.

(c) **Communications Architecture.** Integration requires Link 16 and theater-standard tactical data links, and many C-sUAS systems aren't persistently connected to joint spectrum management networks.

(2) **EMS Conflicts**

(a) **EW Deconfliction.** C-sUAS jamming systems can interfere with friendly communications, GNSS-dependent systems, radar, and other electronic equipment.

(b) **Frequency Coordination.** Integration with HN spectrum authorities and compliance with international frequency allocation agreements is required and complex.

(c) **Mobile Systems.** Ground-based C-sUAS jammers are often mobile and may not be persistently connected to joint spectrum management networks, making real-time deconfliction difficult.

(3) **Sensor Integration Limitations**

(a) **Radar Coverage.** Traditional IAMD systems designed for larger, high-speed threats struggle to detect low, slow, sUAS targets below most AD radar coverage.

(b) **Multinational Sensor Fusion.** Requires fusion nodes at theater air operations centers, national air operations centers, and tactical levels with different data formats.

b. **Procedural Interoperability Challenges**

(1) **Engagement Authorities and ROE**

(a) **Varying Authority Levels.** Different nations may have more restrictive ROE than US unilateral ROE in multinational operations.

(b) **Engagement Zone Coordination.** Coordinated engagement zones needed to prevent friendly fire between US, HN, and allied C-sUAS effectors. Multinational missile engagement zone (MEZ) coordination must account for overlapping national AD zones.

(c) **Pre-delegated Authorities.** Compressed engagement timelines require pre-delegated authorities, but multinational partners may have different approval processes.

(2) **Airspace Control and Management**

(a) **ACM Coordination.** C-sUAS engagement zones need to be deconflicted with theater air operations, adjacent installation C-sUAS operations, and HN territorial defense missions.

(b) **ACO/ATO Integration.** C-sUAS operations in multinational theaters need to synchronize with established ACO production cycles (typically 72-96 hours), which may not align with dynamic threat timelines.

(c) **MEZ/Fighter Engagement Zone (FEZ)/JEZ Coordination.** Multinational operations require integration with different national IAMD architectures. Buffer zones at MEZ boundaries between US and allied systems are needed.

(3) **Information Sharing**

(a) **Classification Management.** Over-classification impedes multinational effectiveness. Need to establish appropriate classification levels that enable sharing while protecting sources and methods.

(b) **Intelligence Sharing Protocols.** Threat intelligence requires near real time sharing, but enemy adaptation timelines (2-to-4-week cycles) outpace many formal intelligence sharing processes.

(c) **Technical Data Exchange.** Sharing control frequencies, signatures, and vulnerabilities require secure frameworks.

(4) **HN Coordination**

(a) **SOFA Limitations.** SOFAs, HN laws, and bilateral security agreements impose additional restraints on C-sUAS operations in specific countries.

(b) **Sovereign Territory.** Engagement of sUAS over HN sovereign territory (outside US installation boundaries) typically requires HN approval, except in cases of imminent threat.

(c) **Base Defense Integration.** Integration with HN territorial defense forces, military police, or facility protection units requires clear US/HN responsibility delineation.

(5) **Training and Standards**

(a) **Different Identification Procedures.** Multinational partners employ different C-sUASs with varying identification capabilities, increasing fratricide risk.

(b) **Interoperability Testing.** Technology transfer to partners requires testing interoperability with existing multinational C-sUAS architecture before operational employment.

(c) **Tactics and Procedures.** Need forums for sharing C-sUAS TTP. The Ukraine conflict demonstrated that successful multinational operations depend on sustained engagement and mutual adaptation as technologies evolve.

c. **Cross-Domain Integration Challenges**

(1) **Joint Fires Coordination**

(a) **Sensor-to-Shooter Integration.** C-sUAS operations require integration of air, ground, maritime, space, and cyberspace sensors. Coordination of kinetic and non-kinetic weapons across domains is complex.

(b) **Fighter Integration.** Coordinating fighter employment against UASs with ground-based C-sUASs requires clear responsibilities and airspace deconfliction.

d. **All-Domain Synchronization**

(1) **Land.** Integration with security forces, EOD, and perimeter security requires reporting procedures integrated into BDOC COP.

(2) **Cyberspace.** Installation network defense must coordinate with theater cyberspace operations to ensure installation-level actions don't conflict with theater campaigns.

(3) **Maritime.** Landing force C-sUAS capabilities on amphibious warfare ships require proper division of airspace and hand-off ranges between systems.

e. **Key Observations from Recent C-sUAS Operations.** There is no single technical or procedural solution to achieving interoperability. Instead, successful C-sUAS operations require:

(1) Modular, open architecture systems with standardized interfaces.

(2) Continuous coordination mechanisms (e.g., working groups, liaison officers, combined planning cells).

(3) Pre-coordinated engagement authorities and procedures rehearsed across

multinational formations.

(4) Acceptance that the threat evolves in 2-to-4-week cycles, requiring continuous adaptation faster than formal doctrine can update.

(5) Sustained engagement, information sharing, and rapid mutual adaptation as threats and technologies evolve.

7. (U) Allied and Multinational Interoperability

a. **Information-Sharing Protocols.** Multinational (alliance or coalition) C-sUAS operations should share information on successful and unsuccessful tactics in a timely manner.

(1) **Threat Intelligence.** Establish protocols for rapid sharing of sUAS threat information among multinational partners. Enemy adaptation timelines require near real time intelligence sharing.

(2) **Technical Data.** Share technical data on UASs, including control frequencies, signatures, and vulnerabilities. This enables partners to optimize their C-sUAS operations.

(3) **Tactics and Procedures.** Establish forums for sharing C-sUAS TTP. Ukraine demonstrated the value of multinational symposiums and subject matter expert exchanges for sharing sUAS lessons learned.

(4) **Classification Management.** Establish appropriate classification levels that enable sharing while protecting sources and methods. Over-classification impedes multinational effectiveness.

b. **Combined Engagement Procedures.** Multinational forces should establish clear procedures for combined C-sUAS operations.

(1) **Engagement Authorities.** Define engagement authorities for each multinational partner, ensuring clarity about who can engage what threats under what circumstances.

(2) **Identification Procedures.** Establish common identification procedures to prevent friendly fire incidents. This is particularly challenging when multinational partners employ different C-sUAS systems with varying identification capabilities.

(3) **Airspace Coordination.** Develop ACMs that accommodate different national systems and procedures. The concept of MEZ/FEZ/JEZ requires adaptation to counter UASs.

(4) **Communications Integration.** Establish secure communications that enable coordination across multinational partners. This includes both voice communications and data sharing for COP.

(5) **EMS Management.** It is critical to deconflict the use of US C-sUAS radar

and C2 systems against allied and partner radar systems within respective RF bands.

c. **Technology Transfer Considerations.** Multinational operations often involve technology-sharing to enhance partner C-sUAS capabilities.

(1) **Security Considerations.** Assess technology security implications before transfer. Balance operational benefit against technology protection requirements.

(2) **Sustainment Planning.** Ensure partners can sustain transferred technology. This includes spare parts, maintenance capabilities, and technical expertise.

(3) **Training Integration.** Coordinate training for transferred systems, ensuring partners can effectively employ new capabilities.

(4) **Interoperability Testing.** Test interoperability of transferred systems with existing multinational C-sUAS architecture before operational employment.

(5) **Capability Coalition Models**

(a) The Electromagnetic Warfare Capability Coalition is a model for pooling resources among nations to advance research, development, and equipment acquisition in the field of EW. By collaborating and sharing resources, participating countries can accelerate the development and deployment of cutting-edge EW capabilities. This coalition approach enables nations to stay ahead of evolving threats and technologies, ensuring a more effective and efficient use of resources. This approach can also be used with C-sUAS efforts. By working together, coalition members can develop and implement C-sUAS capabilities and methods, enhancing their ability to disrupt and counter enemy UASs.

(b) Multinational C-sUAS operations require continuous coordination and adaptation. Establish standing coordination mechanisms (e.g., working groups, liaison officers, combined planning cells) to maintain multinational effectiveness as threats and technologies evolve. The Ukraine conflict demonstrated that successful multinational operations depend on sustained engagement, information sharing, and mutual adaptation to emerging challenges.

d. (U) **Multinational IAMD Architecture Integration**

(1) In theaters with established multinational IAMD architectures (e.g., NATO, coalition operations), C-sUAS operations must integrate with combined AD C2 systems. The theater AADC coordinates C-sUAS operations through the appropriate combined/coalition air operations center, ensuring synchronization with multinational air C2 systems.

(2) C-sUAS sensor data must feed into both national and multinational COPs. US forces integrate C-sUAS tracks using Link 16 and theater-standard interfaces, enabling shared SA across all IAMD nodes.

(3) **MEZ/FEZ/JEZ Coordination in Multinational Operations.**

Multinational weapons engagement zone (WEZ) coordination requires integration with allied national IAMD systems.

(a) Multinational MEZ coordination must account for overlapping national AD zones, particularly in regions where multiple allied SHORAD [short-range air defense] systems operate in proximity.

(b) The theater AADC establishes buffer zones at MEZ boundaries between US and allied systems to enable cross-boundary engagement authorities during high-tempo sUAS attacks.

(c) JEZ employment in multinational operations requires combined/coalition air component commander approval when integrating allied fighter aircraft with US surface-based C-sUAS operations.

(4) **ACO/ATO Integration.** C-sUAS operations in multinational theaters must synchronize with established ACO production cycles.

(a) C-sUAS ACMs are submitted through the theater air operations center ATO production cycle, typically 72-96 hours prior to execution.

(b) Dynamic C-sUAS ROZ requests are coordinated through the senior airspace control authority (ACA), with notification to affected allied air operations centers.

CHAPTER V
LAYERED COUNTER-SMALL UNMANNED AIRCRAFT SYSTEM DEFENSE

Joint Force Commanders (JFCs) plan for defense-in-depth, employing successive layers of C-sUAS capability to overlap area and local defense asset coverage and mitigate dead spaces. The defense should ensure mutual support, be capable of increasing coverage as the threat UASs approach (number and density of C-sUAS assets increase as range to protected asset decreases) and enable integration of complementary supporting systems.

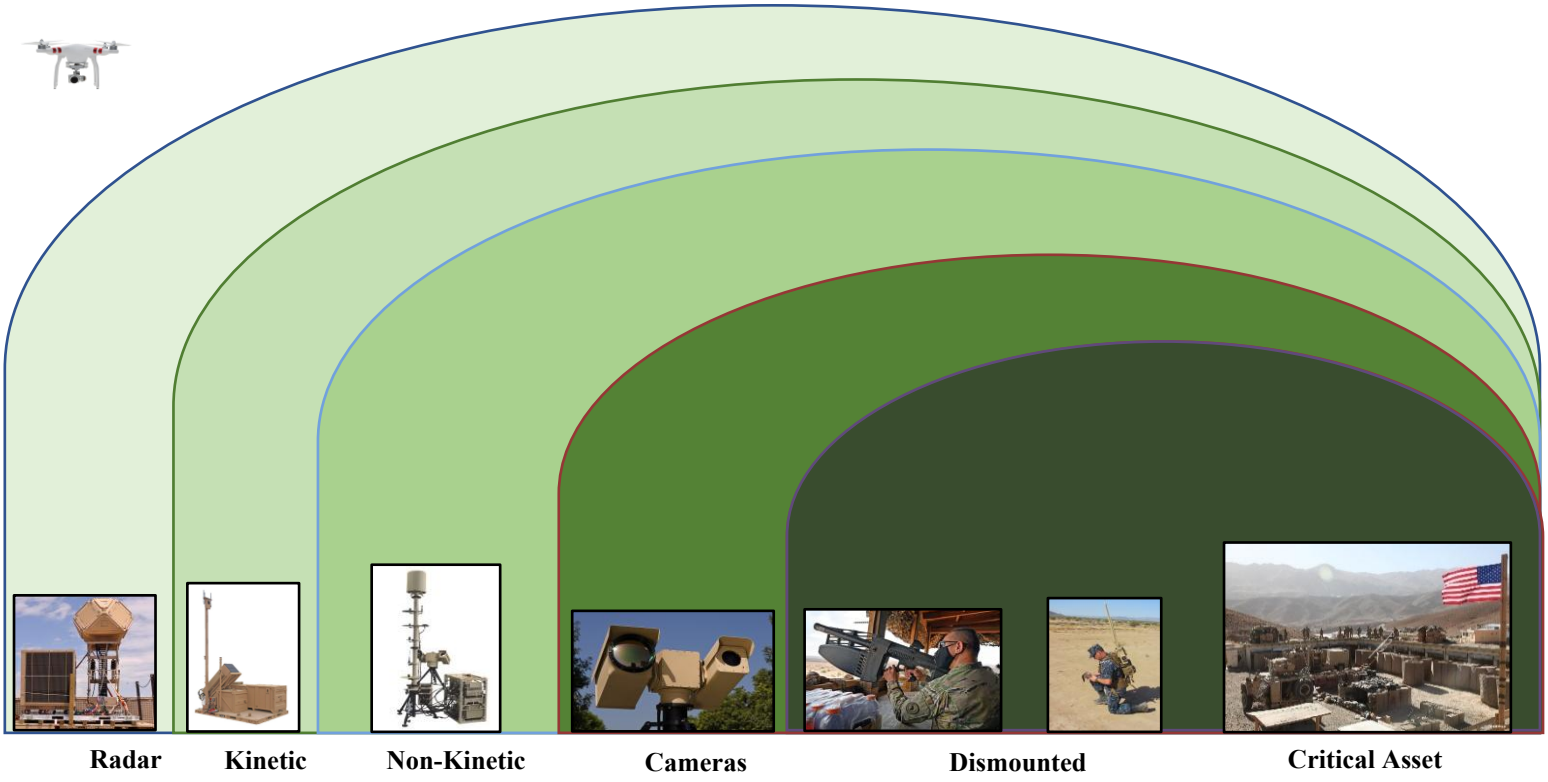


Figure. C-SUAS Layered Defense Strategy

A C-sUAS Layered Defense Strategy combines area and local defense assets, provides dead-space coverage, integrates multiple co-located, C-sUASs, and ensures coverage increases as sUAS threats approach.

1. Responsibilities

Commanders and staff execute C-sUAS activities as part of an overall protection plan, employing the five principles of protection—comprehensive, integrated, layered, redundant, and enduring.

a. **Comprehensive protection** is an all-inclusive use of complementary and reinforcing protection tasks and systems available to commanders and incorporated into the plan to preserve the force.

b. **Integrated protection** is unified with other activities, systems, efforts, and capabilities associated with the conduct of land operations to shape security environments, prevent conflict, prevail in-ground combat, and consolidate gains across the competition continuum. Integration must occur vertically and horizontally with all mission partners throughout operations.

c. **Layered protection** capabilities are sequenced across multiple domains to eliminate, mitigate, or accept the risk of the threat.

d. **Redundant protection** efforts for critical vulnerabilities require primary and alternate protection capabilities.

e. **Enduring protection** is a continuous activity. Commanders preserve combat power and reduce the risk of loss, damage, or injury to their formations.

f. Units should develop and refine C-sUAS training tailored to the expected threat environment. Individual and collective tasks need to be identified, planned, and rehearsed through live, virtual, and constructive training methods and evaluated during training exercises.

2. Prior-to-Launch Mitigation

a. The most effective and cost-efficient C-sUAS action is one that prevents the enemy from launching UA. Prior-to-launch mitigation encompasses intelligence-driven activities to identify, locate, and neutralize enemy sUAS capabilities before employment. This includes targeting the enemy's sUAS infrastructure, including operator networks, supply chains, manufacturing sites, and assembly and modification facilities, and for larger UASs, launch sites, ground control stations, and C2 infrastructure.

b. Prior-to-launch activities span the competition continuum. In competition, they include intelligence collection on enemy sUAS procurement and capabilities and law enforcement actions against illicit sUAS supply networks. In armed conflict, they include kinetic and non-kinetic fires against sUAS assembly sites, launch sites, ground control stations, and storage facilities, as well as special operations targeting of enemy UsAS operator networks. United States Special Operations Command plays an integral role in prior-to-launch activities that target networks enabling sUAS proliferation.

c. **Integration with Theater Deep Strike Planning**

(1) Small UAS infrastructure targets should be integrated into the CCDR's joint

integrated prioritized target list, with priority comparable to AD and logistics nodes based on threat assessment.

(a) **Launch sites and operator positions.** Tactical targets requiring responsive strike capabilities and integration with special operations forces for direct action missions.

(2) **Battle Damage Assessment.** Battle damage assessment for sUAS facility strikes requires multi-intelligence fusion (e.g., geospatial intelligence, SIGINT, human intelligence) due to rapid enemy reconstitution capabilities. Battle damage assessment timelines should account for facility type (i.e., 14-30 days for forward facilities, 60-90 days for production centers).

(3) **Special Operations Forces Integration.** Theater special operations commands conduct prior-to-launch operations targeting enemy sUAS operator networks.

(a) Priority intelligence collection on enemy sUAS training facilities to identify operator cadre for targeting.

(b) Coordination with partner-nation special operations forces for direct action against enemy sUAS ground control stations, particularly high-value operator teams.

(c) Information operations targeting enemy sUAS operator morale and technical competence, exploiting decentralized training structures and limited operator proficiency.

3. Detection, Tracking, and Identification

a. Detection, tracking, and identification of UASs follows the C-sUAS operations cycle framework.

b. **Detect.** Detection is dependent on the ability of sensors to sense the presence of UASs. Commanders use the full depth and breadth of available intelligence and sensors to minimize blind spots that permit the enemy to operate undetected. Intelligence can analyze UASs from a system's perspective and may be able to provide indicators and warning intelligence that enable commanders to make risk-informed decisions. Intelligence that is integrated into the C-sUAS operation's cycle extends the defensive layer and provides decision space for the commander. Sensors can use multiple means of detecting enemy UA and range from humans using their eyes and ears to motion detectors; passive SIGINT and acoustic systems; radars; and other active sensors employed by land, maritime, air, or space platforms. Detection is a critical component of C-sUAS operations. Fast and accurate multi-sensor fusion is essential for UASs, enabling for real-time tracking, identification, and targeting of enemy UASs.

(1) **Types and Limitations of Detection Sensors.** While various sensors may detect an aerial object, detecting UASs pose several challenges. C-sUAS operations may employ one or more of the following sensor types:

(a) **Human Sensors.** The eye is far less capable than technological sensors, as eyes are limited by LOS, range, and light level. Pilots often use their eyes to detect larger UASs. Hearing is also far less capable than technological systems. The human ear can only detect certain decibel ranges, and sound wave propagation often results in inaccurate assessments of bearing.

(b) **RF Sensors.** RF sensors passively scan for radio signals used to control UA or transmit telemetry or video feeds. These systems analyze the technical characteristics of those signals to determine whether they match known sUAS signature profiles. However, some RF detection systems rely on a preprogrammed library, and if the enemy sUAS is operating at a frequency that is not in the library, then the sUAS may go undetected.

(c) **Radars.** Radars are constrained by the radar horizon, radar resolution cell, clutter and the closeness of the object to the earth, the number of contacts, and the reflectivity of the target. Even for advanced radar systems, the primary challenge is discrimination. Discrimination requires the ability to discern UASs from other aerial objects (e.g., friendly UASs, birds, balloons, decoys, debris).

(d) **Cellular Network Sensors.** Some UASs rely on a cellular network for control, and these networks have detectable signals. If the threat sUAS uses a cellular network, the ability to discern the threat from other traffic is inherently challenging.

(e) **Acoustic Sensors.** Some systems use acoustic detection to identify the distinctive sound signatures of sUAS engines and propellers. This method detects airborne objects based on sound patterns, particularly in environments that limit radar or RF detection. Acoustic sensors may identify the library of known audio signatures but can alert on false positives of acoustic noise. Small UASs are difficult to detect acoustically due to the noise profile of electric motors. The Ukrainians have had success against the Shahed UASs due to their louder noise signature.

(f) **EO-IR Sensors.** EO-IR sensors may initially detect or visually confirm the presence of a sUAS. These sensors assist in classification and tracking airborne objects. EO-IR sensors may be limited by LOS, false positives like birds and other airborne clutter, or adversarial EW (i.e., jamming).

(2) **Counter-sUAS Signals Analysis.** Although there are other methods, UASs communicate with their controllers primarily through signals analysis. This signals analysis is limited to detection for those UASs which transmit through the air (radio or cellular). Fiber-optic cables defeat this analysis, as do most AI-controlled missions. C-sUAS detection systems analyze signals through:

(a) **Detecting RF Signatures.** This includes scanning for radio signals used to control UASs.

(b) **Analyzing Waveforms.** This includes examining the unique shapes and patterns of signals to distinguish them from other RF sources such as Wi-Fi and Bluetooth.

(c) **Identifying Characteristics.** This includes measuring frequency, signal strength, bandwidth, power levels, modulation type, and timing.

(d) **Direction Finding/Triangulation.** This includes using multiple antennas and signal processing algorithms to determine the direction, location, and movement of the UA or its controller.

(3) Detection of sUASs is the foundational challenge of sUAS defense. The small size, low radar cross-section, slow speed, and low altitude of small UASs make them difficult to detect with AD radars. Detection is even more challenging for small UASs that are resting on the ground alongside a travel route, often obscured by ground cover, without motors running but with video active to detect targets. C-sUAS detection requires a multi-sensor approach that combines radar, EO-IR sensors, RF detection, and acoustic sensors.

(4) Radar systems optimized for C-sUASs employ shorter wavelengths and specialized processing to detect small targets in ground clutter. However, radar alone cannot identify whether a detected target is a hostile sUAS, a friendly sUAS, a bird, or other small airborne object. EO-IR sensors provide visual identification but are limited by range, weather, and field of view. RF detection systems identify small UASs by their control link emissions but are ineffective against fiber-optic or fully autonomous systems that do not emit in the RF spectrum. Acoustic sensors detect the distinctive sound signatures of multi-rotor UASs but have limited range and are degraded by ambient noise.

(5) Sensor fusion, enabled by automated processing and machine learning, increases the probability of detection, reduces false alarm rates, and provides the identification confidence necessary to support engagement decisions for UASs which can be tracked electronically. Track management systems need to be capable of tracking large numbers of targets in high-density sUAS threat environments.

(6) **Multinational and Theater Sensor Integration**

(a) **Theater-Level Sensor Integration.** In theaters with established air surveillance networks, C-sUAS operations should integrate with theater-level sensors for wide-area detection and cueing.

1. Theater airborne ISR platforms (RQ-4, P-8, E-3, allied equivalents) provide wide-area sUAS detection capability with tracks disseminated via Link 16 to tactical sensors for cueing.

2. Integration with theater air surveillance radar networks provides gap-filler coverage in areas not covered by tactical sensors, particularly for low-altitude contacts and approaches from enemy territory.

3. Space-based sensors provide an additional detection layer for larger UASs and launch point identification.

(b) **HN and Allied Sensor Coordination**

1. Integration of US C-sUAS sensors with HN air surveillance networks provides comprehensive airspace coverage. US C-sUAS tracks should be shared with HN air operations centers via Link 16 or theater-standardized data formats.

2. HN sensors provide cueing to US C-sUASs for tracks detected by national sensors, particularly low-altitude contacts below US radar coverage.

3. Coordination with allied AD fire control radars (Patriot, SAMP/T [Sol-Air Futurs Sol-Air Moyenne-Portée/Terrestre, the French mobile, medium-range SAM], NASAMS) provides additional sensor layer for Group 3 UAS detection.

(c) **Terrain-Specific Acoustic Sensor Employment**

1. Acoustic sensor employment effectiveness varies significantly by terrain type.

a. Forested terrain provides reduced ambient noise and increased detection ranges compared to urban or open terrain but requires adjusted sensor spacing to account for acoustic attenuation.

b. Mountainous terrain creates radar shadows requiring supplemental coverage. Acoustic sensors positioned to cover approach corridors can be used along with electro-optical sensors to provide supplemental coverage.

2. **Acoustic Sensor Network Design Considerations**

a. Integration with seismic sensors to detect ground-launched UASs and discriminate from wildlife.

b. Acoustic library development for theater-specific s UAS threats, as acoustic signatures vary by platform type and environmental conditions.

c. Seasonal calibration of sensor algorithms to account for environmental changes (e.g., foliage, snow cover, temperature inversions).

(d) **Multinational Sensor Fusion Architecture**

1. Multinational operations require fusion of US, allied, and HN sensor data into unified a COP.

a. **Primary fusion node.** Theater air operations center, integrating Link 16 or theater-standardized data formats.

b. **Secondary fusion nodes.** National air operations centers with bilateral data sharing agreements.

c. **Tactical fusion.** US brigade and battalion C-sUAS systems fuse organic sensors with higher-echelon tracks received via tactical data links.

2. **Data Standardization Requirements**

a. US C-sUAS sensors should output tracks in both Link 16 and theater-standard formats for multinational interoperability.

b. Track quality metadata (e.g., sensor type, confidence level, track age) must be preserved across fusion nodes to enable engagement decision making.

c. Common track numbering across US and allied systems prevents duplicate engagements and enables coordinated fires.

c. **Track.** Tracking an enemy UA may entail tracking a larger, high-altitude UA that is emitting an electromagnetic signature and vulnerable to radar detection, or this may entail tracking a small UA at low altitude, with a low radar signature that does not emit an electromagnetic signature. The ability to maintain an unbroken track may also require multiple friendly systems working in concert. Tracking UA requires the ability to share SA of UA from one sector to another; this requires a COP and shared understanding between units and echelons of command. For example, a Service member may visually acquire a small UA and communicate its location and direction of travel to an agency responsible for controlling a target tracking radar, or a SIGINT collection team may acquire a signal that positively correlates to a known enemy UA. They communicate the location to a C-sUAS team optimized for the identified enemy UA. Lastly, the JFC determines which type of fires (kinetic or non-kinetic) to employ to achieve lethal or nonlethal effects.

d. **Identify.** Once a sensor is tracking an enemy UA, operators analyze that data to identify the specific attributes of the sUAS. The type of sUAS provides useful information pertaining to the sUAS's capabilities but more importantly its vulnerabilities. This information is critical to determining the best types of fires to achieve the desired lethal or nonlethal effects. While performing this analysis, it is equally important to maintain target custody by maintaining track on the UA. Identification of enemy UA can be made easier with shared SA and positive friendly identification of friendly UA. Examples of this include friendly force trackers; secure attritable IFF [identification, friend or foe]; and micro-transponders for high-value UA.

4. Engagement and Defeat

Engaging and defeating UASs involve layered defense and can combine both kinetic and non-kinetic fires engagement. The selection of the appropriate defeat mechanism(s) depends on the threat type, defended asset, ROE, electromagnetic environment, and available systems.

a. **Kinetic Fires.** Kinetic fires used to defeat UASs include purpose-built C-sUAS interceptor missiles, gun systems, and shotgun-type systems for close-range engagement. Kinetic fires provide a high probability of kill but are constrained by magazine depth and cost-per-round. They are the primary option against fiber-optic and autonomous UASs that are resistant to EA.

(1) **DE.** High-energy laser systems and high-powered microwave systems offer the potential for low cost-per-engagement and effectively unlimited magazines (constrained by power supply, not ammunition). High-energy laser systems engage targets

with a focused beam of light that damages or destroys the sUAS airframe or components. High-powered microwave systems emit electromagnetic pulses that disrupt or destroy the sUAS electronics. Both technologies face operational limitations, including atmospheric effects on lasers, power generation requirements, and dwell time needed to achieve target effects.

(2) **Non-Kinetic Fires.** EA is the primary non-kinetic fires for RF and GNSS-dependent UASs. Jamming the control link can sever the operator's connection to the aircraft. Jamming satellite navigation denies UASs the ability to navigate to the target. Protocol exploitation injects false commands to redirect or land the sUAS. EW is most effective against COTS and RF-controlled platforms. It is ineffective against fiber-optic-controlled and fully autonomous systems. Employment requires deconfliction with friendly electronic systems. Findings from Ukraine emphasize the need for agile EW capabilities that can adapt quickly to emerging threats. They also underscore the importance of maintaining kinetic fires to counter UASs that are less susceptible to EW capabilities. This includes "final mile" UASs that capitalize on AI to fly autonomously a target, thereby overcoming countermeasures such as EW. The joint force can further use EA, jamming, cyberspace attack, and electromagnetic pulse effects to disrupt or destroy UASs.

(3) **C-sUAS Interceptors.** Friendly UASs can be employed to intercept enemy UASs through direct physical impact, firing weapons, net capture, or EA. C-sUASs offer the advantage of engaging the threat in the air without the collateral risk of ground-based kinetic fire systems. Active protective measures are defensive actions taken to destroy, neutralize, or reduce the effectiveness of threats against friendly forces and assets. Planners should develop multiple options using various combinations of systems, WEZs, and tactics allowing the flexibility to defend critical assets.

(a) Small, mobile teams are a low-cost, high-impact AD solution that add defensive depth.

b. **Dispersion.** Dispersion minimizes the effects of a successful attack by putting fewer people at a location, lessening or confusing the electronic signature to decrease the likelihood of using emissions as a target discriminator, and decreasing the time required to resume normal operations. Disperse as much as possible on installations; use continuity of operation sites; and work with the HN for possible alternate locations as allowed by agreement, HN laws, and international law. Disperse key equipment as well (e.g., move high-value aircraft around available parking locations as frequently as required by the enemy's observation capability).

5. All-Domain Fires Integration (Sensors)

C-sUAS fires should be integrated across all available domains and systems. Ground-based AD systems, direct fire weapons, aviation assets, naval close-in weapon systems, and EW systems all contribute to the layered defense. Sensor integration is a key enabler; sharing track data across all sensor types and echelons ensures the best-positioned shooter(s) engages each threat. The integration of C-sUAS sensors into the broader AMD and C2 architecture enables cross-domain engagement solutions and prevents gaps in the defensive coverage.

6. Engagement Authorities

a. The compressed timelines of C-sUAS engagements require pre-delegated authorities and clearly defined engagement criteria. Commanders should establish weapons control status (WCS), engagement zones, and ROE that enable operators to engage sUAS threats without requiring real-time approval from higher echelons. Commanders should train and rehearse the detect-identify-track-engage-assess kill web supported by automated decision aids to present engagement recommendations to operators in the time available.

b. Engagement authority frameworks need to account for the risk of fratricide against friendly UASs, collateral damage to civilian populations and infrastructure, and the electromagnetic effects on friendly systems. Positive identification requirements must balance the need for certainty against the time constraints of the threat.

7. All-Domain Integration at Force Protection and Base Defense Level

a. Installation C-sUAS operations require integration across all domains to achieve defense against sUAS threats. BDOCs coordinate C-sUAS employment with ground security forces, airfield operations, EW systems, cyberspace capabilities, and information operations to create a layered, mutually supporting defense.

b. **Ground Domain Integration**

(1) Security forces provide ground-based response to C-sUAS engagements.

(a) Quick reaction forces respond to landed or crashed UASs for site security, evidence preservation, and coordination with EOD and intelligence personnel for exploitation.

(b) Perimeter security forces provide visual observation and reporting of sUAS launch, recovery, and ground control station activities in vicinity of installation, with reporting procedures integrated into the BDOC COP.

(c) Security forces establish ground-based observation posts at likely sUAS ingress corridors based on terrain analysis, previous sUAS activity pattern analysis, and enemy tactics assessment, providing an early warning layer for the C-sUAS sensor network.

(d) Security forces conduct response operations to locate and apprehend sUAS operators when UASs are engaged within range-enabling operator location through back-azimuth analysis or RF direction-finding.

(2) **EOD Integration**

(a) EOD provides render-safe procedures for landed UASs with suspected explosive payloads, chemical payloads, or unknown payload configurations.

(b) EOD conducts technical exploitation of recovered sUAS systems to

identify enemy capabilities, tactics, and technical modifications, with exploitation results disseminated to theater intelligence and JIATF-401 for joint force lessons learned.

(c) EOD advises the BDOC on sUAS payload indicators based on flight profile analysis (i.e., OWA sUAS profile versus reconnaissance profile) and platform characteristics (i.e., payload capacity, observed modifications).

c. **Air Domain Coordination**

(1) **Airfield Operations Integration**

(a) C-sUAS sensors provide sUAS track data to air traffic control (ATC) for aircraft flight safety and airspace deconfliction, with tracks displayed on ATC displays where technical integration exists.

(b) Airfield operations implement procedures for flight operations suspension during active C-sUAS engagements when required by safety considerations, with decision criteria and notification procedures established in installation airfield operations instructions.

(c) C-sUAS engagement zones are deconflicted with aircraft approach/departure corridors, published instrument procedures and visual flight rules traffic patterns, and published in airfield operations notices to airmen and installation flying safety publications.

(d) Airfield operations coordinate sUAS hazard reporting to the FAA (for CONUS installations) or HN civil aviation authorities (for OCONUS installations), per established reporting procedures.

(2) **Theater AD Coordination**

(a) Installation C-sUAS operations coordinate with theater IAMD systems operating in vicinity of the installation through the theater air operations center coordination cell, ensuring engagement deconfliction and preventing simultaneous engagement of same sUAS by multiple systems.

(b) The BDOC receives cueing from theater air surveillance sensors (e.g., theater air surveillance radars, airborne early warning aircraft, space-based sensors) for sUAS tracks approaching installation areas, providing extended warning time beyond organic sensor detection ranges.

(c) Installation C-sUAS engagement authority is coordinated with the theater AADC through published SHORADEZ in theater ACO to prevent engagement conflicts with theater AD operations and enable decentralized execution at installation level.

d. **Cyberspace Domain Employment**

(1) **Network Defense Against sUAS Cyber Threats**

(a) Installation network defense monitors for enemy sUAS conducting SIGINT collection against installation networks, network reconnaissance for cyberspace attack planning, or employment of onboard cyber exploitation payloads.

(b) Cybersecurity personnel analyze recovered UASs for cyberspace exploitation capabilities, including Wi-Fi penetration tools, cellular network mapping equipment, RF spectrum collection systems, or network intrusion payloads, with findings reported to theater cyberspace operations.

(c) Installation network defense implements protective measures against sUAS-enabled cyberspace threats, including wireless network security enhancements, RF emission control during elevated sUAS threat periods, and monitoring for sUAS-associated network reconnaissance indicators.

(2) **Offensive Cyberspace Operations Against Small UAS C2**

(a) When authorized by appropriate authority and coordinated through theater cyberspace operations, installation cyberspace operations personnel target enemy sUAS ground control stations, C2 networks, and cellular-controlled sUAS communication links.

(b) Coordination with theater cyberspace operations ensures installation-level cyberspace actions support theater cyberspace campaign plans and do not conflict with theater-level cyberspace operations or intelligence collection operations.

e. **EMS Operations**

(1) **EW Integration with C-sUAS Operations**

(a) Installation EW systems provide C-sUAS effects through jamming of sUAS control links (e.g., RF control, cellular control) and GNSS denial to disrupt sUAS navigation, with employment coordinated through the BDOC to synchronize with kinetic effector employment.

(b) EW systems conduct RF direction-finding operations to locate enemy sUAS ground control stations for targeting by security forces, fires systems, or theater strike assets, with location data disseminated via the BDOC to appropriate response elements.

(c) The BDOC coordinates EW employment with C-sUAS kinetic effectors to prevent electromagnetic fratricide of friendly interceptor UASs, with EW activation/deactivation procedures synchronized with interceptor sUAS employment timelines.

(d) Installation EW personnel analyze recovered UASs for electromagnetic characteristics, including control link frequencies, frequency-hopping patterns, GNSS receiver characteristics, and EW resistance features, to inform EW system employment and update EW databases.

(2) **Spectrum Deconfliction**

(a) C-sUAS EW employment is deconflicted with installation communications systems, ATC radios, navigation aids (e.g., ILS [instrument landing system], VOR [VHF Omnidirectional Range], TACAN [tactical air navigation]), and radar systems through the installation spectrum management office using joint restricted frequency list procedures.

(b) The installation spectrum manager coordinates C-sUAS EW frequencies with HN spectrum authorities to ensure compliance with HN spectrum regulations and international frequency allocation agreements.

(c) C-sUAS EW systems employ directional antennas and power management where feasible to minimize EMI with friendly systems while maintaining effectiveness against sUAS threats.

f. **Information Environment Operations**

(1) **Deterrence Messaging**

(a) Installation public affairs coordinates with HN authorities on public messaging regarding installation C-sUAS capabilities and legal consequences for unauthorized sUAS operations in installation restricted areas.

(b) Visible C-sUAS system deployment (where operational security permits) serves as deterrent to enemy sUAS reconnaissance and attack planning, with public affairs messaging emphasizing defensive capabilities.

(2) **Enemy UAS Operator Targeting**

(a) Intelligence personnel analyze sUAS employment patterns to identify enemy operator locations, tactics, and operational patterns for targeting by security forces, fires systems, or information operations.

(b) Information operations target enemy sUAS operator networks with messaging regarding legal consequences of sUAS operations against US installations, technical countermeasures capabilities, and successful engagement results to degrade operator morale and effectiveness.

(c) Coordination with HN law enforcement enables targeting of enemy sUAS operators through HN legal authorities where sUAS operations violate HN laws.

(3) **Post-Incident Information Operations**

(a) Following successful C-sUAS engagements, coordinated public affairs and information operations messaging emphasizes installation defense capabilities to deter future attacks while maintaining operational security regarding specific C-sUAS tactics and techniques.

(b) Exploitation of recovered sUASs provides information operations

content regarding enemy capabilities, intentions, and operational patterns for use in deterrence messaging and enemy operator targeting.

g. **BDOC Coordination Procedures**

(1) The BDOC maintains coordination with representatives from all domains to enable integrated C-sUAS operations.

(a) **Security forces liaison** for ground response coordination, site exploitation, and operator location operations.

(b) **Airfield operations liaison** for flight safety deconfliction, airspace coordination, and aircraft operations integration.

(c) **EW officer** for EMS coordination, jamming employment synchronization, and direction-finding operations.

(d) **Cyberspace operations liaison** for cyber threat integration, offensive cyberspace operations coordination, and network defense.

(e) **Intelligence officer** for threat analysis, enemy tactics updates, pattern analysis, and exploitation coordination.

(f) **Public affairs representative** for information operations coordination and public messaging.

(2) The BDOC conducts multi-domain C-sUAS rehearsals, integrating all-domain capabilities to ensure coordinated execution during actual sUAS threats, with rehearsals addressing:

(a) Detection and identification procedures across all sensor types.

(b) Engagement decision making and coordination across kinetic and non-kinetic fires.

(c) Post-engagement response, including site exploitation, intelligence reporting, and reconstitution.

(d) Coordination procedures with theater air operations center, adjacent installations, and HN authorities.

(3) Installation commanders should establish multi-domain C-sUAS working groups to synchronize planning, training, and capability development across all-domain representatives, ensuring unity of effort in installation C-sUAS operations.

CHAPTER VI
AIRSPACE CONTROL

1. Introduction

Airspace control and airspace management are critical for the successful employment of joint forces, particularly in an environment saturated with friendly, neutral, and hostile sUASs. The proliferation of these systems, especially at lower altitudes, presents a significant challenge to deconfliction and integrated AD. This chapter provides guidance on integrating C-sUAS operations with traditional airspace control functions. It addresses the necessary integration with AD, AMD, and counterair; the deconfliction of EW effects; and the application of coordination measures to safely and effectively conduct both friendly sUAS and C-sUAS operations.

2. Airspace Control and Airspace Management

a. The term "airspace control" consists of two categories—airspace control and airspace management. **Airspace control** deals with the exercise of delegated authority over designated airspace and users through control procedures and coordination measures to maximize operational effectiveness. **Airspace management** deals with the planning, coordination, integration, and regulation of airspace in support of airspace control.

b. The ACA establishes an ACS [airspace control system] responsive to the needs of the JFC and integrates with outside organizations, as appropriate. The ACS is an arrangement of organizations, personnel, policies, procedures, and facilities required to perform airspace control functions. The ACP [airspace control plan] is designed to identify all airspace users, facilitate the engagement of hostile air and missile threats, and expedite safe passage of friendly and neutral aerial platforms. ACOs provide specific airspace control procedures applicable for defined periods based on the general guidance of the ACP. ACOs are designed to deconflict planned airspace usage and help identify airspace users. The ACO provides the details of the approved requests for coordination measures and is published either as part of the ATO or as a separate document.

c. **Planning Considerations for UA.** The established principles of airspace control used in manned flight operations normally apply to sUAS operations. However, small sUASs may be difficult to detect due to their small physical size, low-altitude operations, low radar cross-section, lack of IFF transponder, or weak electromagnetic emissions (passive detection), presenting a potential hazard to other aircraft. For the same reasons, positive identification may be difficult. Therefore, friendly sUASs and C-sUAS operations require special considerations in terms of airspace control and management. Specific sUAS volumes of airspace should be included in the ACO. Additionally, the ACO should provide times of activation of airspace for sUAS operations. In cases where a standing ACO is used, specific details are addressed in the ATO or SPINS [special instructions]. In either case, the agency (i.e., owner) responsible for a specific portion of airspace is responsible for integrating manned and unmanned aviation. For example, if the ACA assigns airspace to a United States Army division to perform procedural control, then the division is responsible for integration within the assigned airspace boundaries. Efforts

should be made to integrate sUASs with manned flight operations to enable a more flexible and adaptable airspace structure.

(1) While the C2 of friendly sUAS operations are similar to those for manned assets, several characteristics of sUASs can make C2 particularly challenging. Furthermore, friendly and enemy sUASs share similar characteristics. Thus, the ability to C2 friendly sUAS operations while simultaneously conducting C-sUAS operations can be incredibly challenging.

(2) The volume of friendly sUAS operations juxtaposed with the volume of C-sUAS operations requires detailed coordination between the ACA AADC. For example, the AADC needs to be aware of all airspace control documents (e.g., ACP, ACO, ATO, SPINS), while the ACA needs to be aware of all AMD documents. The ability to conduct friendly sUAS operations that are integrated with AMD and C-sUAS operations are vital to mission success.

Refer to JP 3-52, Joint Airspace Control, *for more details on airspace control.*

3. Air Defense Warning and Level/Modes of Control

a. The JFC normally designates a component commander as the AADC to be the overall commander for DCA operations, and typically, this commander is also designated by the JFC as the JFACC [joint force air component commander]. The AADC is responsible for planning, coordinating, and integrating the joint force's AMD operations. This responsibility includes the development and implementation of the area air defense plan (AADP), which synchronizes all active ADs, passive defense measures, and associated C2 architecture. A critical function of the AADC within this role is the dissemination of timely threat warnings to the force. Centralized control and decentralized execution are key C2 considerations when organizing for joint air operations. To enable decentralized execution, the AADC normally delegates some or all AADC authorities down to the RADC [regional air defense commander] or SADC [sector air defense commander] level (if established). The AADC specifies the conditions and limits within which engagement authority is decentralized. Based upon the threat level and the complexity of engagements, a control node should retain engagement authority at the level where airspace management can be adequately performed. For airspace management, the AADC or a RADC/SADC uses three tools for which the authorities may be delegated further down to the tactical level—air defense warning conditions (ADWCs), WCS, and fire control orders. These control measures should be adapted for the C-sUAS environment where the threat may be persistent rather than episodic, requiring sustained elevated postures that stress crew endurance and system readiness. Engagement authority controls are normally delegated at the tactical level in accordance with the supported commander's guidance, as specified in the AADP.

b. **ADWCs.** While the ADWC system is the standard for communicating theater-level threats, its application to localized C-sUAS threats requires careful consideration. A single sUAS detected over a patrol base, for example, may not warrant escalating the ADWC for the entire joint operations area. Therefore, the AADP should account for the need for localized warning systems and procedures. These local warnings provide the across the theater, and the authority to issue them may be delegated to local commanders.

c. The challenge of accurately identifying sUASs is significant. These systems often have a minimal radar cross-section and are difficult to distinguish from clutter, birds, or friendly sUASs. Therefore, robust target identification procedures and clear ROE are paramount to reduce friendly fire and minimize collateral damage. The AADC, in coordination with the ACA and other component commanders, is responsible for developing and disseminating these C-sUAS-specific ROE. These ROE should provide guidance on HN sensitivities, criteria for engagement, and who has the authority to engage hostile sUASs within various airspace regimes.

d. An AD warning, which includes missile attacks, is issued as an ADWC. The ADWC is a degree of air attack probability based on the threat assessment. The AADC establishes the baseline ADWCs for the joint force. ADWC levels may be different for various threats. RADCs/SADCs may issue higher but not lower ADWCs for their areas. ADWCs are disseminated though joint and component C2 channels to all AMD elements and fire units.

(1) ADWC White—An attack by hostile aircraft or missile is improbable.

(2) ADWC Yellow—An attack by hostile aircraft or missile is probable.

(3) ADWC Red—An attack by hostile aircraft or missile is imminent or in progress.

(4) A change to an ADWC should not automatically prescribe a specific action. Consider the following actions and force posture changes with changes to ADWC:

(a) Weapons readiness.

(b) Alert posture.

(c) WCS.

(d) Engagement criteria.

(e) Asset positioning (e.g., AMD units, combat air patrols, and high-value airborne asset retrograde).

(f) Alert aircraft (e.g., launch, upgrade posture).
(g) Deny targeting (e.g., emissions control, decoys).

e. **WCS.** WCS is a control measure that establishes the conditions under which manned aircraft and surface AMD weapons (including small arms) are permitted to engage threats. The AADC establishes WCS for the joint force. The WCS may be different for various threats. WCS authority originates with the AADC and can be delegated to subordinate commanders. Different WCSs may be applied simultaneously to different weapons systems and in different airspace areas. US forces use three standard WCSs that may be declared for a particular area and time. The WCSs are free, tight, and hold. Generally, US forces disseminate WCS via voice and tactical chat and not tactical data link. WCS dissemination means should be addressed in the AADP and amplifying guidance (e.g., SPINS, fragmentary orders). The transition between WCSs in response to a sUAS threat should be rehearsed and pre-coordinated. Standing operating

procedures should define the specific conditions under which WCS changes are authorized and at what echelon that authority resides.

(1) **Weapons Free.** The least restrictive status; when any target not positively identified as friendly in accordance with current ROE may be engaged. Weapons free zones may be established around key government infrastructure when other areas are designated weapons tight or weapons hold.

(2) **Weapons Tight.** The normal status. Units may only fire on targets identified as hostile in accordance with current ROE. Note: Weapons free and weapons tight control orders impose a status or condition applicable to weapons systems within a defined volume of airspace, and normally, any unit directly threatened by a missile of any type, friend or foe, may engage it.

(3) **Weapons Hold.** The most restrictive status. Units may only fire in self-defense or when ordered by proper higher authority.

f. **Fire Control Orders.** Fire control orders address both air and missile threats and standardize tactical firing instructions issued during an air battle. They are given to direct or inhibit firing by surface-to-air weapons units based on the ROE and rapidly changing tactical situations. Based on the ROE, the JFC-approved AADP should establish how fire control orders are communicated. There are three primary fire control orders—engage, cease engagement or cease fire, and hold fire.

g. **Level of Control.** Level of control describes the echelon where airspace management occurs. This can be at AADC; RADC; SADC; or AD artillery brigade, battalion, or the weapon system itself, based on capability. Different levels of control are usually established for fixed-wing, rotary-wing, and sUAS engagements.

h. **Modes of Control.** Joint forces require familiarity with the overall area AD plan, which specifies the modes of control, trigger events, when they should be changed, and who has the authority to change them. The selected mode of control may depend on the capabilities of the communications system, the weapons systems employed, and both the friendly and enemy air situation. The three modes of control for AMD are centralized, decentralized, and autonomous.

(1) **Centralized Control Mode.** In this mode, a higher echelon authorizes target engagement by a firing unit.

(2) **Decentralized Control Mode.** In this mode, a higher echelon monitors unit actions. It makes direct target assignments on a management-by-exception basis to ensure proper fire distribution, prevent engagement of friendly air platforms, and prevent simultaneous engagement of hostile air targets.

(3) **Autonomous Operations.** A unit assumes autonomous operations after losing all communications with higher and adjacent echelons. The unit commander assumes full responsibility for control of weapons and engagement of hostile targets. Typically, the ROE and supplemental fire control measures in effect at the time of communication loss remain in effect until communications are regained. Changes to ROE

and supplemental fire control measures scheduled to go into effect after communications are lost are implemented as scheduled.

4. Integration with Integrated Air and Missile Defense and Counterair

a. **IAMD** is the broad joint approach to defending the force against all air and missile threats. It integrates and synchronizes offensive and defensive actions to attain and maintain a desired degree of control of the air. Joint IAMD integrates capabilities and overlapping operations to defend the homeland and US national interests, protect the joint force, and enable freedom of action by negating an enemy's ability to create adverse effects from their air and missile capabilities. IAMD incorporates offensive and defensive measures to create a comprehensive joint and combined force capable of preventing an enemy from effectively employing its offensive air and missile weapons. IAMD is designed to deter and, failing that, prevent an enemy from effectively employing air and missile assets.

b. **Counterair**, which consists of OCA and DCA missions, is the primary means by which IAMD is executed. Since hostile sUASs are air threats, C-sUAS operations should be understood and executed as a fundamental component of the counterair fight and fully integrated into the broader IAMD architecture.

c. **IAMD systems** were not originally designed to address low, slow, and small targets operating at altitudes below most AD radar coverage and at speeds that may not trigger engagement criteria designed for faster threats. Integration requires that C-sUAS sensors feed track data into the IAMD COP. C-sUAS engagement zones must be deconflicted with AD engagement zones to prevent mutual interference. C-sUAS capabilities operating in the same airspace as IAMD systems must be coordinated through the AADC and the ACA.

(1) The integration of C-sUASs into the counterair framework involves both offensive and defensive actions. OCA missions, in the context of C-sUASs, focus on preventing the launch of hostile sUASs by attacking or disrupting their supporting infrastructure. This includes targeting sUASs ground control stations, launch and recovery sites, and the operators themselves. Within a theater, IAMD is primarily focused on DCA, which involves actively defeating hostile sUASs that are airborne. AMD is also directly supported by OCA operations providing protection for US and partner forces. This is accomplished using a range of kinetic and non-kinetic fires. A comprehensive C-sUAS strategy requires the deliberate planning and synchronization of both OCA and DCA efforts to counter the threat at all phases of its employment.

(2) Figure VI-1 depicts the relationship between counterair as the foundational framework at the theater level and IAMD as the vertical integrating approach between counterair and global missile defense, homeland defense, global strike, and countering indirect fire. Suppression of enemy ADs, fighter sweeps, and fighter escorts are shown as counterair missions outside of the IAMD approach.

(3) The integration of dedicated C-sUAS capabilities into the established IAMD framework presents significant challenges. Traditional IAMD systems, designed to counter larger, high-speed threats like aircraft and missiles, are often ill-suited for the low

and slow and small UAS threat, and, if not mobile, are particularly vulnerable to them. Their sensors may struggle to detect or track these targets, and their high-cost interceptors are not a sustainable solution for countering low-cost UASs. Furthermore, the proliferation of C-sUAS sensors can overwhelm C2 systems with data, cluttering the common tactical picture and straining the decision-making process. The AADP therefore accounts for these challenges by integrating appropriate C-sUAS capabilities and establishing clear procedures to enable rapid engagement.

(4) To overcome these integration hurdles, C-sUAS capabilities are developed and procured using a system-of-systems approach. This requires the enforcement of open architecture principles, common data standards, and standardized interfaces. By doing so, new C-sUAS capabilities are more easily integrated into the broader IAMD framework, allowing them to share data seamlessly across the joint force. This approach ensures the overall C-sUAS architecture is adaptable, scalable, and resilient enough to meet the evolving threat.

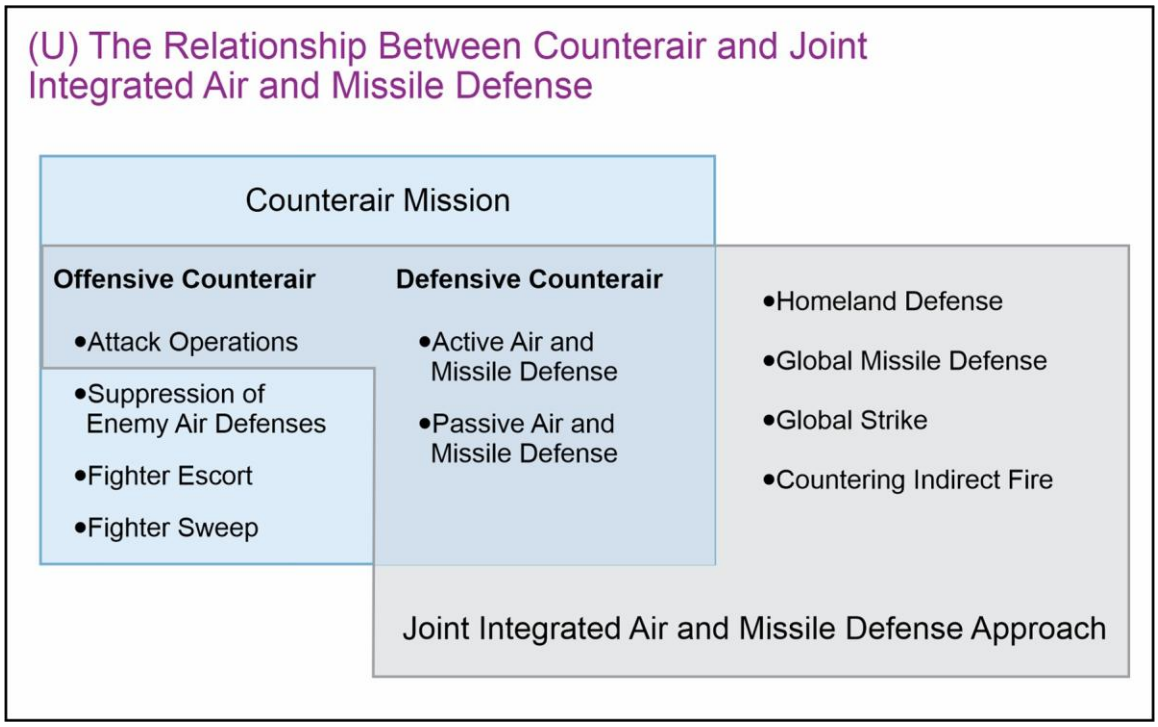


Figure. The Relationship Between Counterair and Joint Integrated Air and Missile Defense

(5) **Multinational AMD Integration.** In multinational operations, C-sUAS capabilities integrate with combined layered AMD architecture.

(a) US C-sUASs coordinate with theater missile defense architecture, particularly when defending strategic assets against combined sUAS and missile threats.

(b) C-sUAS engagement zones are deconflicted with allied AD systems (Patriot, SAMP/T, NASAMS) through the multinational COP.

(c) US forces employ standardized multinational identification procedures

for C-sUAS operations to prevent fratricide across multinational formations.

(6) A particularly difficult challenge is the threat of massed, coordinated attacks by swarms of hostile UA. Traditional IAMD architectures are designed to engage a limited number of high-performance threats and can be quickly saturated by a large volume of low-cost, small UA. The AADP should therefore evolve to account for this threat, incorporating systems and TTP capable of managing mass engagements and prioritizing threats within a swarm. This may require leveraging AI to automate the detection, tracking, and engagement process.

Refer to JP 3-01, Countering Air and Missile Threats, for more details on joint IAMD and counterair.

(7) **Coordination Measures.** Coordination measures are employed to facilitate the efficient use of airspace to accomplish missions and, simultaneously, provide safeguards for friendly forces. A coordination measure commonly used in AMD is a WEZ. A WEZ is airspace of defined dimensions within which the responsibility for engagement of air and missile threats normally rests with a particular weapons system. There are three types of WEZs.

(a) **FEZ** is that airspace of defined dimensions within which the responsibility for engagement of air threats normally rests with fighter aircraft.

(b) **MEZ** is that airspace of defined dimensions within which the responsibility for engagement of air and missile threats rests with ground AD units. A MEZ is established to defend critical assets, protect maneuver units in the forward area, and provide area coverage for the rear areas. There are three types of MEZs.

1. **HIMEZ [high-altitude missile engagement zone]** is airspace of defined dimensions within which the responsibility for engaging air and missile threats, including endo- and exo-atmospheric BMs, rests with high-altitude SAMs (e.g., SM [standard missile]-3, SM-6, THAAD [Terminal High Altitude Area Defense]).

2. **LOMEZ [low-altitude missile engagement zone]** is airspace of defined dimensions within which the responsibility for engagement of air and missile threats rests with low- to medium-altitude SAMs (e.g., SM-2, Patriot). This is the airspace where larger UASs typically operate.

3. **SHORADEZ** is airspace of defined dimensions within which the responsibility for engagement of air and missile threats rests with SHORAD weapons (e.g., Avenger). This is the airspace where small UASs typically operate.

(c) **JEZ** is airspace of defined dimensions within which multiple AMD systems (i.e., surface-to-air and aircraft) are simultaneously employed to engage air and missile threats. The JEZ construct blends MEZ and FEZ into a more flexible engagement zone, thus increasing combat capabilities. The JEZ coordinates operations against all types of enemy airborne targets concurrently. The FEZ increases capabilities to achieve desired effects of neutralizing sUASs prior to DAL.

(d) **Exploitable Gaps.** Operations along the edges of WEZs, sectors, or other geographically defined areas of airspace with separate controlling units or commands may create seams and present commanders with extensive coordination challenges. Enemy sUASs, particularly Group 3 UASs (e.g., Shahed), operate across a broad range of mission altitudes. This ability provides enemy sUASs the flexibility to select operating altitudes that traverse the boundary between LOMEZs and SHORADEZs. If the coordination between engagement authorities for the various MEZs is lacking, an exploitable gap can emerge that enables enemy sUASs to achieve their mission. Enemy sUASs may cross into adjacent sectors during engagement, fly through friendly corridors, or attack targets in one area from an adjacent area. The following are some considerations to facilitate coordination:

(e) Airspace Control

1. Establish procedures to coordinate handovers of flight operations between sectors and regions. These procedures should grant permissions to enter and depart airspace and coordinate combat zone control activities with HN ATC services. A dedicated communications network dividing line between regions and sectors is necessary to enable rapid handovers.

2. Liaison officers should be placed at ATC centers providing positive control for areas overlapping or adjacent to AMD areas.

3. Designate buffer zones in which one AMD region or sector can authorize an engagement in an adjacent area.

4. Whenever possible, establish friendly air corridors outside the ranges of friendly AMD forces which rely only on visual identification, to reduce the risk of friendly fire. Visually aimed surface weapons often have no capability to identify airspace boundaries or control measures in their portion of the OA. Together, the ACA and AADC should plan to address these issues.

5. Electromagnetic Attack Deconfliction

a. EA is a central component of many C-sUAS operations, which often use EA to disrupt the link between a hostile UA and its operator. While highly effective, the employment of these C-sUAS EA systems creates a significant risk of EMI with friendly C2 systems, communications, and navigation capabilities. Therefore, the deconfliction of friendly C-sUAS EW systems from other operations within the EMS is a planning consideration that addresses pre-coordinated and authorized RF allocations to prevent electronic friendly fire and ensure mission success.

b. The JFC has overall responsibility for the JEMSO [joint electromagnetic spectrum operations] and manages and controls the EMS within the joint operations area. To execute this responsibility, the JFC normally establishes a JEMSOC or a similar joint spectrum management element within the staff. This entity is the central point of contact for coordinating spectrum requirements and deconflicting electromagnetic systems for all components. All C-sUAS operations that have the potential to create EMI must be coordinated with and deconflicted through this joint spectrum management element.

c. EA is used in C-sUAS operations, but it creates electromagnetic effects that effect other systems. Counter-sUAS jamming systems can interfere with friendly communications, GNSS-dependent systems, radar, and other electronic equipment. JEMSO, per JP 3-85, *Joint Electromagnetic Spectrum Operations,* provide the framework for managing these competing demands. EA deconfliction for counter-sUAS operations requires coordination. The JEMSOC or equivalent staff element maintains awareness of all C-sUAS EA systems, their frequencies of operation, effective ranges, and planned employment windows. Deconfliction addresses both spatial separation (i.e., ensuring C-sUAS jamming does not affect friendly systems in adjacent areas) and temporal separation (i.e., scheduling C-sUAS EA employment to avoid conflict with critical friendly electromagnetic activities). The fundamental tension in C-sUAS EA is that the most effective non-kinetic fires operate in the same spectrum that friendly forces depend on for C2, navigation, and SA. Resolving this tension requires spectrum management and disciplined EW employment procedures.

d. The deconfliction of C-sUAS EA systems presents unique and significant challenges. C-sUAS capabilities often consist of numerous, diverse, and geographically dispersed systems from various vendors. Many of these systems are mobile, creating dynamic and unpredictable bubbles of potential EMI. Furthermore, because hostile commercial sUASs often use the same common frequencies as friendly forces (e.g., satellite navigation, Wi-Fi), C-sUAS EA systems may disrupt friendly command, control, and navigation capabilities. These factors complicate deconfliction and require deliberate and detailed planning.

e. The primary source for restricted frequencies is the joint restricted frequency list (JRFL). The JRFL is a tabulated list of frequencies in the OA, classified as PROTECTED, GUARDED, or TABOO. These terms provide guidance on whether they can be targeted by EA. The JRFL also provides the time slots that specific frequencies are needed for operations and are therefore protected from friendly EA. This list includes frequencies used for GNSS, specific satellite communications, and critical air-to-ground communications. All C-sUAS EA systems should be planned and employed in a manner that avoids causing interference with frequencies listed on the JRFL. It is the responsibility of the joint spectrum management element to maintain and disseminate the JRFL to all components.

f. While the JRFL provides a critical baseline for deconfliction, it may not be sufficient to manage the dynamic employment of numerous C-sUAS EA systems at the tactical edge. Ground-based C-sUAS jammers are often mobile and may not be persistently connected to the joint spectrum management network, making real-time, top-down deconfliction difficult. Therefore, units employing C-sUAS EA systems also establish local, procedural deconfliction measures that include direct coordination with adjacent units, clear reporting procedures for when a system is activated, and establishing C-sUAS engagement windows or zones that are understood by affected forces in the immediate area.

g. The deconfliction of C-sUAS EA is not solely a spectrum management issue; it is also an airspace control issue. The effects of C-sUAS EA can create hazards for friendly air platforms by disrupting their navigation and communication systems. Therefore, the known or planned effects of C-sUAS EA systems should be integrated into the ACP.

This is normally accomplished by requesting and publishing ACMs, such as a ROZ, around the area where C-sUAS jamming is authorized. This ACM serves to notify all aircrew that they may experience GNSS or communications interference within the specified airspace, allowing them to plan accordingly and preventing unnecessary emergencies.

h. EA is a key component of the defense. Observations in Ukraine demonstrated the importance of prioritizing EA capabilities and working to mitigate the effects on other operations instead of limiting EW to a non-interference basis. EA cannot be employed on a non-interference basis, it requires prioritized planning and operations to be effective.

i. Airspace Control

Other operations should learn to mitigate the risks of operating in a contested EA environment. EA can disrupt, degrade, deceive, or destroy sUAS control and navigation.

i. EW is used throughout the layers of defense.

(1) Disrupts sUAS navigation to their targets.

(2) Diverts sUASs away from protected areas.

(3) Destruction through loss of communication and crash landing.

6. For Unmanned Aircraft Systems and Counter-Unmanned Aircraft Systems

a. The JFC normally designates the JFACC as the ACA. This authority is central to managing the complex airspace challenges presented by numerous low-altitude UA and C-sUAS activities.

b. The control of airspace is normally achieved through a combination of positive and procedural control measures, which are used to manage and deconflict friendly air assets. Positive control relies on real-time tracking using surveillance systems like radar and IFF. However, due to the low radar cross-section and lack of transponders on most small sUASs, positive control of friendly sUASs operating in the same area is often not feasible. Therefore, the safe operation of friendly UA depends almost exclusively on robust procedural control. This is accomplished through the proactive implementation of ACMs that deconflict air users in time and space.

c. The reliance on procedural control is critical in the airspace where radar coverage is not possible or available, such as below the coordination level (CL). This volume of airspace is normally the maneuver space of the land or maritime component commander and is often a congested, high-risk environment where friendly helicopters,- artillery, mortars, friendly sUASs, and enemy sUASs all operate in close proximity. The lack of positive control and the density of operations in this area means that the land and maritime component commanders must work closely with the ACA to implement appropriate coordination measures to deconflict C-sUAS operations and prevent fratricide.

d. ACMs are employed to facilitate the efficient use of airspace to accomplish

missions and simultaneously provide safeguards for friendly forces. The lack of direct communication between some UA operators and other airspace users frequently requires procedural ACMs to deconflict airspace. The following are common ACMs and FSCMs [fire support coordination measures] used to support sUAS operations:

(1) UA flight corridors and minimum-risk routes channel the flow of friendly UA traffic, while a no-fire area is used to prohibit kinetic fires engagements around sensitive locations. For areas with a high density of air traffic, a high-density airspace control zone enforces specific entry, exit, and operational procedures for all aircraft. Finally, a weapons free zone, which is a type of AD measure around a friendly C-sUAS asset or a defended area, controls all air activity and authorizes specific C-sUAS engagement rules within its boundaries.

(2) A UA ROZ is airspace of defined dimensions created for sUAS operations that permit maximum mission flexibility. This airspace defines where UA missions are conducted and does not include en route airspace. Planners should request sufficient airspace to facilitate unique platform requirements (e.g., sensor performance, turn radius requirements), as well as integrate and coordinate with manned assets for optimal use of airspace.

(3) Kill boxes are control measures consisting of an FSCM and corresponding ACM. UA operating within a kill box may be deconflicted with fires and under the procedural control of the kill box coordinator.

(4) **Air Corridor Used as a Special Corridor.** UA flight routes above the CL should use a special corridor air corridor established by the ACA, based on the mission. Airspace control elements advise all affected aircraft of the special corridor status.

e. **CL.** The CL is a procedural coordinating measure requiring aircraft to coordinate with the airspace control element to transition above or below. A CL allows airspace planners to deconflict low-level routes for rotary-wing and tiltrotor aircraft and small UASs. Friendly UA without self-identification capability (e.g., IFF, Link-16), which are generally sUASs, normally stay below the CL unless mission requirements dictate operating above the CL. Dynamic UA operations below the CL should avoid established ACMs on the ACO (e.g., SAFFR [standard use Army aircraft flight route], LLTR [low-level transit route]). UA operators should not perceive airspace below the CL as an uncontrolled flight area. UA operating below the CL should avoid known SHORADEZs until operators coordinate for, and deconflict, airspace.

f. Complex Civilian Airspace Coordination

(1) **Dense Civilian Air Traffic Environments.** In theaters with dense civilian air traffic and complex airspace structures, C-sUAS operations require enhanced coordination beyond standard military procedures.

(a) C-sUAS ROZ requests affecting civilian airways require coordination through HN civil aviation authorities and regional airspace coordination centers, with minimum 72-hour notice for planned operations.

(b) Dynamic C-sUAS activations near major civilian airports require real-time coordination with civil aviation authorities through established military-civilian coordination cells or liaison officers.

(c) C-sUAS EA employment must comply with civilian frequency protection requirements, particularly for instrument landing system frequencies (108-112 MHz) and VOR navigation aids (108-118 MHz).

(2) **Multinational ACO/ATO Cycle Integration.** C-sUAS operations in multinational theaters synchronize with established ACO/ATO production cycles.

(a) C-sUAS airspace requests are submitted to the theater air operations center not later than 96 hours prior to execution for inclusion in the ACO planning cycle.

(b) Short-notice C-sUAS operations (inside 72 hours) are coordinated through the senior duty officer and published via ACO amendment or time-critical target procedures.

(c) Multinational exercise C-sUAS operations require ACO coordination across multiple national AORs, with lead-nation responsibility assigned by the CCDRs with AORs.

(3) **Multinational Exercise ROZ Procedures**

(a) Exercise C-sUAS ROZ are established using theater-standard formats and include:

1. Activation/deactivation times coordinated across multiple time zones.

2. Multinational entry/exit procedures accommodating different national identification systems.

3. Frequency deconfliction across US, allied, and HN systems.

(b) Large-scale exercise C-sUAS operations (battalion level and above) should employ temporary segregated areas rather than ROZ, providing positive control of all airspace users and reducing coordination complexity.

Refer to JP 3-52, Joint Airspace Control, *and Army Techniques Publication 3-52.1/Marine Corps Reference Publication 3-20F.4/Navy Tactics, Techniques, and Procedures 3-56.4/Air Force Tactics, Techniques, and Procedures 3-2.78, Multi-Service Tactics, Techniques, and Procedures Airspace Control, for more details on airspace control considerations.*

CHAPTER VII
TRAINING AND EDUCATION

1. Overview

a. The rapidly evolving landscape of contemporary warfare has introduced new challenges to IAMD training and operations. Adversaries have demonstrated their ability to use sUASs to their advantage. Unmanned platforms, ranging from advanced military-grade sUASs to simple COTS sUASs repurposed as airborne IEDs, have been used effectively in recent conflicts, including the Russia-Ukraine conflict and Operation EPIC FURY. In the war in Ukraine, sUASs provided persistent battlefield surveillance, enabled precise and low-cost attacks on both military and critical civilian infrastructure, and have been used for sophisticated swarming tactics.

b. Adversaries are rapidly innovating by adapting commercial sUASs and leveraging AI to create a transparent battlefield where standard concealment is no longer as effective. This multi-faceted use of sUASs highlights their potential to disrupt operations and influence outcomes on the battlefield. Adversaries are challenging traditional AD strategies by exploiting vulnerabilities in sensor coverage, target tracking, C2, and magazine depth.

c. The rapid employment of sUASs by adversaries has exposed training deficiencies. Traditional training programs have not sufficiently prepared personnel to identify and classify low, slow, and sUASs, limiting defenders' ability to respond effectively. Counter-**s**UAS operations are fundamentally a force defense and protection task essential for every unit at every echelon, not just a specialized AD mission.

d. The joint force prepares for armed conflict in OAs where sUAS and C-sUAS saturation is permanent, multi-layered, attritional, and embedded in enemy forces. This requires training to prepare the joint force for continuous sensing, a degree of automated decision support, a more integrated AD, and more robust passive and active protection measures.

2. Training Strategy

a. The joint force requires a comprehensive C-sUAS training strategy that builds individual competence, develops collective proficiency, and integrates C-sUAS operations into joint training events. The training strategy needs to address institutional training that produces qualified individuals, unit training that builds collective capability, and joint training that validates integration across the Services. The training needs to synchronize the AD aspects of C-sUAS operations with unit-level force defense and protection functions, rather than treating them as two separate missions.

b. The C-sUAS operations training strategy is nested within the Joint Training System per Chairman of the Joint Chiefs of Staff Instruction 3500.01, *Joint Training Policy for the Armed Forces of the United States.* The Services are responsible for developing training programs that meet CCMD readiness requirements. CCDRs are

responsible for integrating C-sUAS training into theater exercises and pre-deployment preparation. JIATF 401 provides the framework, training standards, and institutional training capacity to support the Services and CCMDs.

c. Operators require specialized training to address emerging threats, focusing on both technical proficiency and cognitive skills.

(1) First, technical proficiency is essential, as personnel must deepen their knowledge in areas such as EW, cyberspace protection, and advanced sensor technology. This includes understanding EA and electromagnetic protection measures; mastering the use of cyberspace protection mechanisms to safeguard critical C2 systems; and becoming proficient with advanced sensors capable of detecting and tracking elusive threats like hypersonic missiles, sophisticated military-grade sUASs, and COTS sUASs. Expanding weapon system knowledge at the tactical level provides defenders with a crucial information advantage.

(2) Second, cognitive skills are crucial for air defenders operating under the intense pressures of modern warfare. Compressed decision-making timelines, leaving little room for hesitation or error, are required for low and slow sUASs, which are often detected late. Training programs need to enhance decision making under stress, improve SA, and develop rapid information-processing skills. Techniques such as high-intensity simulations, real-time strategy exercises, and cognitive resilience training help personnel make swift, accurate decisions in rapidly evolving threat scenarios. Strengthening these cognitive skills better prepares air defenders for contemporary warfare.

3. Joint Counter-Small Unmanned Aircraft Systems University

The Joint Counter-Small Unmanned Aircraft Systems University (JCU) at Fort Sill, Oklahoma, serves as the joint institutional training center for C-sUAS operations. JCU provides formal courses of instruction to operators, maintainers, planners, and leaders from all Services and select interagency partners. JCU curriculum covers C-sUAS operations, employment tactics, integration planning, threat analysis, and legal authorities. JCU is the primary venue for establishing baseline C-sUAS operations competency across the joint force and serves as the doctrinal training arm of JIATF 401.

4. Universal Joint Tasks

Counter-sUAS operations should be reflected in the UJTL [Universal Joint Task List] to enable CCDRs to articulate C-sUAS training requirements, design joint force requirements, and assess readiness. Joint mission-essential tasks specific to C-sUAS operations should address detection and identification of sUAS threats, engagement and defeat of sUASs, integration of C-sUAS operations with AD and force protection operations, and C-sUAS C2. These tasks provide the framework for designing joint training events and measuring C-sUAS operations readiness across the joint force.

For more information on universal joint tasks, see the UJTL Website at https://jdeis.js.smil.mil/jdeis/index.jsp?pindex=43.

5. Joint Knowledge Online

Joint Knowledge Online (JKO) provides distributed learning modules that supplement institutional and unit-level C-sUAS training. JKO courses provide baseline C-sUAS awareness training to the broadest possible audience across the joint force, reaching personnel who may not have access to JCU or unit-level training programs. JKO C-sUAS modules address sUAS threat awareness, basic C-sUAS planning considerations, reporting procedures for sUAS incidents, and C-sUAS TTP. JIATF 401 and JCU worked with JKO to develop and deploy courses aimed at equipping warfighters with the skills needed to counter the small UAS threats.

For more information, see the JKO Website at https://jkolms.jten.smil.mil/Atlas2/page/login/Login.jsf.

6. Joint Professional Military Education

JPME [joint professional military education] institutions need to incorporate C-sUAS doctrine into applicable courses and programs of instruction. C-sUAS education within the joint force starts with the Services but is institutionalized in joint forces through JPME. C-sUAS-specific courses introduce C-sUAS principles at the operational and strategic levels. However, C-sUAS considerations should be integrated into JPME planning scenarios and exercises to build understanding at the operational level of warfare. This inculcates a better understanding for senior leaders who put into practice the knowledge provided in this pamphlet and from other doctrinal sources.

7. New Equipment Fielding and Training

The rapid pace of C-sUAS technology development produces a continuous cycle of new equipment fielding. New equipment training must keep pace with fielding timelines to ensure operators and maintainers are proficient on new systems before they are employed operationally. Training for C-sUASs should include operator qualification, maintainer certification, integration training with existing force protection and AD systems, and tactical employment training against targets. Coordination between acquisition program offices, JIATF 401, and receiving units is essential to synchronize fielding and training schedules.

8. Mobile Training Teams

Mobile training teams (MTTs) extend C-sUAS training capability to operational units and installations that cannot attend centralized courses at JCU. MTTs provide tailored instruction, including system operation, employment tactics, integration planning, and staff synchronization training. MTTs can be deployed to units preparing for deployment, installations implementing new C-sUAS capabilities, or CCMD headquarters requiring C-sUAS planning support. MTTs provide flexibility to deliver training where and when it is needed rather than requiring units to send personnel to a centralized location.

9. Unit-Specific Training

Operational units should develop organic C-sUAS training programs that build and sustain proficiency between institutional training events and deployments. Unit-level C-sUAS training should include individual operator and crew drills, integration of counter-sUASs into unit collective training events, and rehearsals of C-sUAS operations standard operating procedures. Units should incorporate realistic sUAS target representations into their training using approved commercially available training UASs that replicate threat flight profiles and electromagnetic signatures. Unit-level training programs should be informed by the latest threat intelligence and lessons learned from operational deployments.

10. Counter-Unmanned Aircraft System Gunnery Program

The Services should establish standardized C-sUAS gunnery programs, as appropriate, that provide a progressive, structured approach to building and certifying crew and unit proficiency on C-sUAS capabilities. Modeled on existing gunnery standards for direct fire weapons systems, a C-sUAS gunnery program should establish gunnery tables that progress from individual operator tasks through crew qualification to collective engagement scenarios. Gunnery standards should address detection and classification accuracy, engagement timelines, ROE compliance, and integration of multiple C-sUAS capabilities in a layered defense. The Services should adapt their C-sUAS gunnery programs to their specific capabilities and employment concepts while maintaining common standards that support joint interoperability.

11. Services

The Services have increased their sUAS and C-sUAS training over the past few years in response to recent conflicts. Specific C-sUAS training is included below. It is important for the Services to note that C-sUAS operations are not a separate discipline, rather they are inherently a mission set that needs to be synchronized with unit-level protection functions. They are not two separate missions. Equally important, C-sUAS efforts need to synchronize with IAMD as part of the effort to create a layered defense in the OA. Unit-level training needs to focus on realistic, contested scenarios where specialized AD organizations enable and reinforce C-sUAS actions executed by all other C-sUAS-capable units.

a. **United States Army.** The Army's Fires Center of Excellence at Fort Sill, Oklahoma, is the joint force's lead for AD training, experimentation, and doctrine development. The Army recently published Field Manual 3-01, *Army Air and Missile Defense Operations,* which describes the overall AD planning and coordination to counter all groups of UASs. The Army is also revising Army Techniques Publication 3-01.81, *Counter-Unmanned Aircraft System Techniques,* which goes into depth regarding both the planning considerations for defending against sUASs during operations, as well as how to plan for and incorporate C-sUAS tasks into unit training for tactical forces (brigade level and below).

b. **United States Marine Corps.** The Marine Corps has published the *Organic Counter Small Unmanned System Concept of Employment* and is developing the Organic Counter-Small Unmanned Aircraft Systems family of systems designed to enable the movement, maneuver, and protection of distributed naval expeditionary forces by countering threat sUASs from all adversaries. In addition to the fielding effort, it has a corresponding systematic strategy for C-sUAS training.

c. **United States Navy.** The Naval Air Warfare Center, Weapons Division, provides advanced C-sUAS training within the Navy and Marine Corps. Their comprehensive training programs, realistic training environments, and ongoing experimentation prepare personnel to counter the evolving sUAS threat. The Naval Air Warfare Center, Weapons Division, is located at Naval Air Weapons Station, China Lake, California. They offer the C-sUAS [Counter-Small, Unmanned Aircraft System] Basic Operator course, which is a foundational course, and the C-sUAS Advanced Operator course, building on the basic operator course.

d. **United States Air Force.** The Air Combat Command established the Point Defense Battle Lab as a collaboration hub for a series of exercises focused on improving how the United States Air Force defends its installations against sUASs. The lab includes a team to develop and validate enhanced TTP for protecting US military installations from sUASs.

e. **National Guard Bureau**

(1) Oklahoma Army National Guard operates a dedicated C-sUAS school, training military personnel alongside industry partners to enhance mission readiness against sUAS threats. The training focuses on detecting, identifying, and mitigating sUAS threats, while integrating with Air Force and Army components in comprehensive, joint force defense. The goal of the training is to provide personnel with the knowledge and skills necessary to detect, identify, track, assess, respond to, and report sUAS activity.

(2) Recent reports of unauthorized sUAS sightings near sensitive US military installations and critical infrastructure have raised national security concerns. These incidents highlight vulnerabilities to potential surveillance, espionage or even weaponized sUAS attacks and emphasize the need for enhanced C-sUAS technology and training programs for military and law enforcement personnel to detect, identify, and neutralize sUAS threats, safeguarding national assets and preventing potential harm. The National Guard Bureau is assessing integration of mobile C-sUAS capabilities into the weapons of mass destruction civil support teams for the prevention of and response to potential sUAS chemical, biological, or radiological hazard delivery in the homeland.

f. As the joint force moves forward, opportunities to conduct C-sUAS training with multinational forces OCONUS are beneficial. The United States Army Center for Army Lessons Learned published “Eyes on the Horizon: Honing Counter Drone Skills in Eastern Europe” (February 2026). This document has a thorough discussion on establishing a C-sUAS training environment in an HN. It identifies the following nine key actions:

(1) HN permissions.

(2) HN agreements.

(3) Integrate stakeholders into planning.

(4) Identify sUASs and C-sUASs units will use.

(5) Select the training site.

(6) Submit spectrum requests.

(7) Deconflict air space.

(8) Establish real-world C-sUAS force protection measures.

(9) Coordinate sustainment.

12. Interagency

The FBI recently established the National Counter-Unmanned Aircraft System Training Center in Alabama for state and local law enforcement personnel. It certifies law enforcement officers to conduct domestic C-sUAS operations as deputized FBI task force officers, able to operate under their own authority once Department of Justice regulation is implemented. Furthermore, the Department of Homeland Security is in the process of standing up a course at the Federal Law Enforcement Training Centers for federal operators.

13. Allies and Partners

C-sUAS Fundamentals Training Course (NATO). In support of NATO's ongoing efforts to strengthen C-sUAS capabilities, the Joint Air Power Competence Centre developed a C-sUAS course tailored for the NATO C-sUAS community of interest. It is offered monthly to members across all ranks of the NATO C-sUAS community, including relevant law enforcement agencies and critical infrastructure stakeholders. In addition, NATO offers three specific recommendations when training units and organizations beyond the individually focused training conducted during the course and highlights suggested future changes in AD doctrine.

a. **Incorporate Realistic Threat Simulations.** Joint exercises with allies should incorporate realistic threat simulations enabled by current technology to foster best practices, information sharing, and collaborative readiness.

b. **Enhance Intelligence Sharing.** Strengthening intelligence sharing among western nations is crucial to staying ahead of emerging threats. Platforms such as BICES [Battlefield Information Collection and Exploitation System] enable seamless information exchange among NATO members, while multinational intelligence cells dedicated to emerging threats ensure training programs remain informed by updated intelligence.

c. **Train for Interoperability.** Cross-Service and cross-domain integration is essential for a cohesive defense strategy; training air defenders in cyberspace and space

operations enhances their understanding of modern warfare's interconnected domains. Joint training with international partners strengthens collective readiness, while multinational exercises like NATO's Joint Warrior and the Technical Interoperability Exercise events improve coordination and interoperability, as well as operational cohesion among allies and partners.

d. **Theater and Multinational Training Integration**

(1) **CCMD Theater Training.** CCDRs should consider integrating C-sUAS training into theater exercise programs.

(a) MTT deployment to rotational force locations on cycles synchronized with unit rotations, addressing theater-specific challenges, including terrain, HN airspace coordination, multinational ROE, and civilian ATC coordination requirements.

(b) Coordination with HN training facilities for C-sUAS live-fire training, including airspace coordination procedures and range safety requirements.

(2) **Multinational Exercise Integration.** Major theater exercises should incorporate C-sUAS as integrated component.

(a) C-sUAS systems deploy with rotational forces and conduct live training during reception, staging, onward movement, and integration phases at HN training areas.

(b) Multinational C-sUAS integration exercises focusing on interoperability, COP development, and scenario-based training replicating observed enemy employment patterns.

(c) Standardized exercise C-sUAS training objectives across theater exercises.

1. Multinational sensor integration and track sharing.

2. Coordinated engagement procedures across US and allied systems.

3. Airspace coordination with theater ACO/ATO cycles.

4. EW deconfliction across multiple national systems.

5. HN coordination procedures for sovereign airspace.

(3) **Allied Training Coordination.** Integration with allied C-sUAS training programs enables cross-training and interoperable procedure development.

(a) Participation in allied C-sUAS courses and communities of interest for sharing TTP across multinational partners.

(b) Multinational operator exchanges (30-60-day rotations) enable cross-training on allied systems and development of interoperable procedures.

(c) Quarterly coordination forums for sharing lessons learned and threat

updates across allied forces.

14. Adaptation by North Atlantic Treaty Organization Allies

a. NATO Allies are implementing new training programs, integrating advanced technologies, and developing innovative tactics to counter sUAS threats.

(1) The German Air Force has recently incorporated hypersonic threat trajectories into its training simulations, enabling personnel to practice detection and interception in realistic scenarios. Regular intelligence briefings update threat assessments, while collaborative workshops with defense agencies drive innovation in counter-hypersonic strategies. Limited access to detailed threat data remains a challenge, highlighting the need for improved intelligence-sharing mechanisms within NATO frameworks, such as the BICES network.

(2) The Netherlands' Defense Ground-based Air Defense Command addresses emerging IAMD threats through advanced courses such as the Patriot Advanced Capability course and Weapon Instructor course. They partner with scientists and knowledge institutes to stay ahead of technological developments, ensuring lessons learned from recent conflicts, including Ukraine, are integrated into their national training programs. The Dutch Army also employs passive defense measures such as mobility and decoys to complicate enemy targeting and ensure survivability.

(3) Australia has also emphasized emerging technologies in training and operations. Their forces highlight the importance of decentralized command structures, allowing lower echelons to make rapid decisions in dynamic threat environments. Additionally, interagency cooperation strengthens readiness across military branches and civilian agencies.

b. These adaptations highlight the importance of innovation, flexibility, and continuous learning in countering sUAS threats. By incorporating real-world insights and unconventional tactics into training and operations, NATO Allies can refine their IAMD capabilities to address the complexities of modern warfare.

15. Exercises, Experimentation, and Simulations

a. The joint force Elite Constellation Campaign uses an OA built to reflect the breadth of joint functions and all-domain operations. Accuracy, coherence, and true-to-form conditions are designed in campaign events to ensure the joint force lessons learned can be rapidly applied. The design uses current and emergent joint force capabilities, tactics, and techniques which allows the joint force to rapidly adapt as lessons are learned.

b. Both enemy and friendly use of sUASs has advanced rapidly and is having an impact on joint operations today. Current model and simulation capabilities used to support Elite Constellation Campaign's OA enable participants to plan and execute sUAS and C-sUAS operations at the operational to strategic levels. The campaign is not focused on the tactical level but does enable operational to strategic sUAS and C-sUAS planning and execution using modelling and simulation, live, virtual, or constructive approaches.

16. Conclusion

a. Adapting training and education is imperative for defending against sUAS threats. Adversaries identify and exploit vulnerabilities in technology and training, making proactive adaptation essential. To stay ahead, air defenders should evolve their TTP in an iterative manner, making their systems and tactics more resilient, unpredictable, and effective against emerging threats. This requires a holistic approach that combines rigorous training, realistic exercises, and information sharing amongst all stakeholders.

b. Incorporating advanced technologies such as AI for real-time threat assessment, predictive analytics, and automated response systems enables defenders to address threats faster and more accurately. This aids human operators where they are not available or lack the necessary reaction time future conflicts demand. Adaptability in tactics is equally important, allowing air defenders to adjust to enemy methods in real time, whether this means employing EW against sUASs or coordinating cyberspace forces to disrupt enemy command networks. By fostering a culture of innovation and adaptability within the IAMD community, NATO can close technological and doctrinal gaps and ensure the security of NATO airspace.

CHAPTER VIII
FUTURE OF COUNTER-SMALL UNMANNED AIRCRAFT SYSTEMS

The evolving threat posed by sUASs, especially sUASs, has fundamentally altered the character of modern warfare, presenting unique challenges to the joint force. Small UASs are inexpensive, widely available, and capable of delivering precision effects that impose significant costs. The integration of AI and other advanced technologies has further enhanced the lethality of all sUASs and increased operational complexity, requiring a comprehensive and adaptive approach to countering this threat. JFCs should consider the following sUAS developments as they plan for a future fight.

1. Autonomous and Artificial Intelligence-Enabled Systems

a. The joint force will leverage advancements in autonomous systems and AI to counter increasingly sophisticated sUAS threats. These technologies will enable the joint force to maintain operational superiority in contested environments by enhancing decision making; improving response times; and enabling dynamic, joint all-domain operations. In addition, considering recent conflicts in Ukraine and in Operation EPIC FURY, there may be opportunity for the JFC to apply data and analytics to refine a joint fires and targeting strategy using AI-enabled applications to provide objective input and accelerate any operational decision making.

b. **Swarming Capabilities**

(1) Swarming, described in this pamphlet as the coordinated action of a mass of unmanned vehicles to achieve a common objective, will become a critical capability for both offensive and defensive operations. The joint force will employ swarms ranging from basic preprogrammed systems to highly advanced, AI-enabled formations capable of dynamic, adaptive operations in complex and unpredictable environments.

2. Directed Energy

DE weapons will serve as a cornerstone of the joint force's C-sUAS capabilities by providing scalable, cost-effective, and precise defensive options as part of an integrated, layered AD. These systems will enable the joint force to counter the proliferation of unmanned systems and maintain freedom of maneuver in contested environments.

a. **Advantages**

(1) DE weapons will provide a low-cost-per-engagement solution compared to traditional missile systems, enabling the joint force to sustain operations in resource-constrained environments.

(2) DE weapons will deliver precise, scalable effects, allowing commanders to tailor engagements to mission requirements.

(3) DE weapons will feature deep magazines, enabling the joint force to engage multiple targets simultaneously without the logistical constraints of traditional munitions.

3. Counter-Unmanned Systems (All-Domain Expansion)

The joint force must prepare to counter enemy sUASs that exploit domain boundaries and physical seams. These systems will challenge traditional defenses and require innovative approaches to detection, tracking, and engagement.

4. Allied and Partner Interoperability

The joint force will enhance collaboration with allies and partners to address the global challenge posed by sUASs. Counter-sUAS operations will require a unified approach that leverages the strengths of allied and partner forces and enables seamless integration in C-sUAS operations. This may include:

a. **Standardized Systems.** The joint force will develop interoperable platforms and communication protocols to enable joint and combined operations.

b. **Shared Intelligence.** Establishing secure data-sharing frameworks will enhance SA and enable rapid identification and engagement of sUAS threats.

c. **Joint Training.** The joint force will conduct multinational exercises to refine TTP for countering unmanned systems, ensuring readiness and cohesion among allied and partner forces.

5. Conclusion

a. By integrating advancements in AI, DE, and allied interoperability, the joint force can maintain a decisive edge in countering the evolving threat posed by sUASs. These capabilities will enable the joint force to operate in contested environments, ensuring mission success and preserving freedom of action across all domains.

b. In addition, the joint force needs to continue efforts to build greater interoperability in the C-sUAS fight. It should build on Service-level efforts such as those described in Navy Tactics, Techniques, and Procedures 3-26.8, *Counter-Small Unmanned Aircraft Systems (C-sUAS),* and Army Techniques Publication 3-01.81/Marine Corps Reference Publication 10-10B.1, *Counter-Small Unmanned Aircraft System (C-sUAS) Operations.* It should also capture the hard-earned lessons of recent combat operations to ensure greater interoperability both within the joint force and with our allies and partners.

c. Countering sUASs spans multiple operations, affects all joint functions, and is a critical part of protecting the force. JP 3-10, *Joint Security Operations in Theater,* will undergo a revision in the summer of 2026. We anticipate a significant change in that publication, to include a greater focus on protection and, as part of that change, a robust discussion of C-sUASs.

APPENDIX
RISKS, LIMITATIONS, AND MITIGATION DURING COUNTER-UNMANNED AIRCRAFT SYSTEM OPERATIONS

1. Operational Risks

a. Threat Characteristics:

(1) Offense-Defense Imbalance. Small UAS favor attackers; cost to produce/employ is a fraction of detection and defeat costs.

(2) Cost-Exchange Challenge. Using multimillion-dollar interceptors against low-cost sUAS creates unsustainable cost ratios.

(3) Saturation Attacks. Mass/swarm tactics are designed to exhaust defensive magazines and overwhelm sensor capacity.

(4) Rapid Adaptation. Enemy's UAS modifications occur in 2-to-4-week cycles, requiring continuous evolution of defensive measures.

(5) Persistent Threat. sUASs enable persistent surveillance, making it difficult to hide force disposition and intentions.

b. Technical Challenges

(1) Detection Difficulties. Small size, low radar cross-section, slow speed, low altitude, and weak electromagnetic emissions make sUASs hard to detect.

(2) Identification Problems. Difficult to distinguish hostile sUAS from friendly sUAS, birds, clutter, or neutral commercial systems.

(3) Autonomous Systems. AI-enabled and fully autonomous sUAS operate without RF emissions, defeating traditional EW.

(4) Sensor Gaps. Traditional IAMD sensors struggle with low, slow, small targets operating below coordination levels.

c. Operational Vulnerabilities

(1) Electromagnetic Fratricide. C-sUAS EW systems can interfere with friendly communications, GNSS, radar, and other systems.

(2) Airspace Complexity. High density of friendly sUAS operations creates identification and deconfliction challenges.

(3) Compressed Timelines. sUAS threats compress engagement timelines to seconds, requiring pre-delegated authorities.

(4) Seams and Gaps. Adversaries exploit boundaries between engagement zones, altitude layers, and adjacent sectors.

(5) Logistics Exposure. Predictable, high-signature logistics nodes are lucrative sUAS targets.

2. Limitations

a. System Limitations

(1) Magazine Depth. Traditional AD systems have limited interceptors; unsustainable

against mass attacks.

(2) Sensor Coverage. Radar shadows, terrain masking, low-altitude gaps, and weather affect sensor performance.

(3) Environmental Factors. Wind, precipitation, visibility, fog, sea clutter, and electromagnetic clutter degrade effectiveness.

(4) Range Constraints. Close-in defenses may lack sufficient warning time for timely engagement.

(5) Interoperability Gaps. Integration challenges between legacy IAMD systems and new C-sUAS capabilities.

b. Operational Constraints

(1) Legal Authorities. Different authorities for homeland verse overseas operations; coordination with FAA, FBI, Department of Homeland Security, and HNs required.

(2) ROE Complexity. Need to balance engagement speed with fratricide prevention and collateral damage mitigation.

(3) Training Gaps. Insufficient preparation for low-altitude, high-density sUAS environments.

(4) Cognitive Overload. Volume of sensor data and track management can overwhelm operators and C2 systems.

(5) Sustainment Challenges. Supply chain vulnerabilities for sensors, effectors, and software updates.

c. Resource Limitations:

(1) Asset Prioritization. Limited C-sUAS resources require difficult choices about what to defend.

(2) Dispersed Operations. Some forces too dispersed or mobile to defend effectively.

(3) EMS Congestion. Competing demands for EMS between C-sUAS, communications, and navigation.

(4) Power Requirements. Directed energy systems require substantial, sustained power generation.

3. Mitigation Strategies

a. Layered Defense Approach

(1) Prior-to-Launch Mitigation (Most Effective)

(a) Target sUAS Infrastructure. Such as factories, supply chains, assembly sites, operator networks.

(b) Deep strike planning against production facilities.

(c) Special operations forces targeting of enemy operator teams and forward staging centers.

(d) Intelligence-driven targeting of sUAS networks (similar to counter-IED operations).

(2) Detection Layer

(a) Multi-Sensor Fusion. radar, EO-IR, acoustic, RF, and space-based sensors.

(b) Networked sensor architecture with automated processing and machine learning.

(c) Low-cost acoustic sensors for early warning at air ingress points.

(d) Integration with theater air surveillance and HN sensors.

(3) Engagement Layer

(a) Kinetic Fires. Guns, interceptor missiles, interceptor sUAS, kinetic intercept.

(b)Non-Kinetic Fires. EW (GNSS denial/spoofing, control link jamming), directed energy (high-energy lasers, high-powered microwave).

(c)Passive Defense. Camouflage, concealment, deception, hardening, dispersion, mobility.

b. Cost-Effective Solutions

(1) Low-Cost Interceptors. Develop systems like LUCAS to counter mass attacks.

(2) Directed Energy. Deep magazines and low cost-per-engagement.

(3) Decoys and Deception. Complicate enemy targeting without expensive technology integration

(4) AI-Enabled Systems. Automated threat assessment, pattern recognition, and engagement recommendations.

(5) Sensor Fusion.Combine radar, EO-IR, acoustic, and RF data for improved detection and identification.

(6) Networked Architecture. COP with standardized data interfaces and plug-and-play capability.

(7) Edge Computing. Process data locally using 5G networks to reduce decision timelines.

c. EMS

(1) JRFL. Protect critical frequencies from friendly EA.

(2) Spatial/Temporal Deconfliction. Coordinate C-sUAS EW employment to avoid interference.

(3) Directional Antennas. Minimize electromagnetic interference footprint.

(4) Prioritized EW Employment. Prioritize GNSS denial/spoofing systems paired with cueing radars.

d. Organizational Approaches

(1) Pre-Delegated Authorities. Enable tactical-level engagement without higher approval

for time-sensitive threats.

(2) Decentralized Execution. Push engagement authority and sensor data to lowest practical echelon.

(3) Unified C2 Architecture. Integrate C-sUAS into IAMD COP.

(4) JEZs. Coordinate surface-to-air and aircraft systems for flexible engagement.

e. Force Protection Measures

(1) Dispersion. Avoid concentration; frequent repositioning of high-value assets.

(2) Layered Engagement Zones.Outer zones (kinetic), inner zones (kinetic/non-kinetic), overlap for redundancy.

(3)Passive Measures. Emission control, hardening, revetments, separation distances.

(4) Rapid Reconstitution.Pre-position materials for quick repair after. strikes.

f. Multinational Coordination

(1) Standardized Procedures.Common identification, engagement authorities, and ACMs.

(2) Intelligence Sharing.Rapid dissemination of threat data, technical characteristics, and TTP.

(3)Interoperable Systems. Link 16, theater-standard data formats, cross-boundary track sharing.

(4)(Combined Training. Multinational exercises to rehearse coordination procedures.

g. Training and Readiness

(1) Realistic Scenarios. Train against fiber-optic, autonomous, and swarm threats.

(2) Cognitive Skills Development. Decision making under stress, compressed timelines.

(3)Gunnery Programs. Structured progression from individual to collective engagement.

(4)Continuous Adaptation. 2-to-4-week enemy adaptation cycles require rapid doctrinal updates.

h. Planning Integration

(1)Joint Planning Process. Embed C-sUAS in mission analysis, COA development, wargaming.

(2)Defended Asset Lists. Prioritize based on criticality, vulnerability, consequence of loss, defendability.

(3)Integration with Fires. Coordinate sUAS infrastructure targeting in joint fires process.

(4)Logistics Planning. Dispersed posture, redundant supply routes, temporal dispersion of high-signature activities.

4. Key Takeaways

a.Most Critical Mitigation. Prior-to-launch targeting of sUAS infrastructure and operator networks provides the best cost-exchange ratio and reduces defensive burden.

b.Foundational Requirement. Multi-sensor fusion and networked C2 architecture are essential for managing volume, velocity, and variety of sUAS threats.

c.Sustainability Challenge. Layered defense combining low-cost solutions (mobile firing teams, directed energy, EW) with selective use of exquisite weapons is necessary to sustain operations against mass attacks.

d.Adaptation Imperative. Enemy adaptation cycles demand continuous intelligence collection, rapid dissemination of lessons learned, and agile modification of TTP.

GLOSSARY

SHORTENED WORD FORMS (ABBREVIATIONS, ACRONYMS, AND INITIALISMS)

AADC	area air defense commander
AADP	area air defense plan
ACA	airspace control authority
ACM	airspace coordination measure
ACO	airspace control order
AD	air defense
ADWC	air defense warning condition
AI	artificial intelligence
AMD	air and missile defense
AOR	area of responsibility
ATC	air traffic control
ATO	air tasking order
BDOC	base defense operations center
BM	ballistic missile
C2	command and control
CBP	Customs and Border Patrol
CCDR	combatant commander
CCMD	combatant command
CL	coordination level
COA	course of action
CONUS	continental United States
COP	common operational picture
COTS	commercial off-the-shelf
C-sUAS	counter-small unmanned aircraft system
C-UAS	counter-unmanned aircraft systems
DCA	defensive counterair
DE	directed energy
DHS	Department of Homeland Security
DoJ	Department of Justice
DoW	Department of War
EA	electromagnetic attack
EMI	electromagnetic interference
EMS	electromagnetic spectrum
EOD	explosive ordnance disposal
EO-IR	electro-optical-infrared
EW	electromagnetic warfare
FAA	Federal Aviation Administration (DOT)
FBI	Federal Bureau of Investigation (DOJ)
FEZ	fighter engagement zone
FPV	first-person view
GNSS	Global Navigation Satellite System
HN	host nation
IAMD	integrated air and missile defense
IED	improvised explosive device
ISIS	Islamic State of Iraq and Syria

ISR	intelligence, surveillance, and reconnaissance
JCU	Joint Counter-Small Unmanned Aircraft Systems University
JDN	joint doctrine note
JEZ	joint engagement zone
JFC	joint force commander
JIATF-401	Joint Interagency Task Force 401
JKO	Joint Knowledge Online
JP	joint publication
JRFL	joint restricted frequency list
km	kilometer
LOS	line of sight
MANET	Mobile Ad Hoc Network
MEZ	missile engagement zone
MTT	mobile training team
NATO	North Atlantic Treaty Organization
OA	operational area
OCA	offensive counterair
OCONUS	outside the continental United States
OWA	one-way attack
RF	radio frequency
ROE	rules of engagement
ROZ	restricted operating zone
SA	situational awareness
SecWar	Secretary of War
SHORADEZ	short-range air defense engagement zone
SIGINT	signals intelligence
SLTT	state, local, tribal, and territorial
SOFA	status-of-forces-agreement
sUAS	small unmanned aircraft system
TCO	transnational criminal organization
TTP	tactics, techniques, and procedures
UA	unmanned aircraft
UAS	unmanned aircraft system
US	United States
USC	United States Code
USCG	United States Coast Guard
USAFRICOM	United States Africa Command
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USNORTHCOM	United States Northern Command
USPACOM	United States Pacific Command
USSOUTHCOM	United States Southern Command
WCS	weapons control status
WEZ	weapons engagement zone

REFERENCES

Air Force Tactics Techniques, and Procedures (ATTP) 3-2.78, Multi-Service Tactics, Techniques, and Procedures Airspace Control, June 2021.

Army Techniques Publication (ATP) 3-01.81, Counter-Unmanned Aircraft Systems (C-sUAS) Operations, May 2025.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3121.01, Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces, June 2005.

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3500.01, Joint Training Policy for the Armed Forces of the United States, November 2024.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3212.02, Performing Electromagnetic Attack in the United States and Canada for Tests, Training, and Exercises, October 1998.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3212.03, Performing Tests, Training, and Exercises Impacting the Global Positioning System, November 2013.

Department of Homeland Security, Science and Technology, Detecting and Mitigating Drones on the Border, April 2025.

Joint Doctrine Note (JDN 1-26), 1-16, Counter Unmanned Aircraft Systems (C-sUAS), July 2026.

Joint Publication (JP), 3-01, Counter Air and Missile Threats, April 2017.

Joint Publication (JP) 3-10, Joint Security Operations in Theater, July 2019.

Joint Publications (JP) 3-27, Homeland Defense, December 2023.

Joint Publication (JP), 3-52, Joint Airspace Control, October 2022.

Joint Publication (JP), 3-85, Joint Electromagnetic Spectrum Operations,

Joint Interagency Task Force (JIATF-401) C-sUAS Quick Reference Guide (QRG), August 2026.

Joint Task Force-Southern Border, Lessons, Reflections, & Observations, Defending the Homeland, 2025.

Marine Corps Reference Publication (MCRP) 3-20F.4, Marine Air Traffic Control, June 2023.

Marine Corps Training and Reference and Operations Group (MCTOG) 10-10, Counter-Unmanned Systems, June 2026.

Navy Tactics, Techniques, and Procedures (NTTP) 3-26.8, Counter-Small Unmanned Aircraft Systems (C-sUAS).

Navy Tactics, Techniques, and Procedures (NTTP) 3-56.4, Airspace Control, 2023.

United States Northern Command and North American Aerospace Command Before the House Armed Services Committee Strategic Forces Subcommittee, March 2026.


JOINT INTERAGENCY TASK FORCE
401