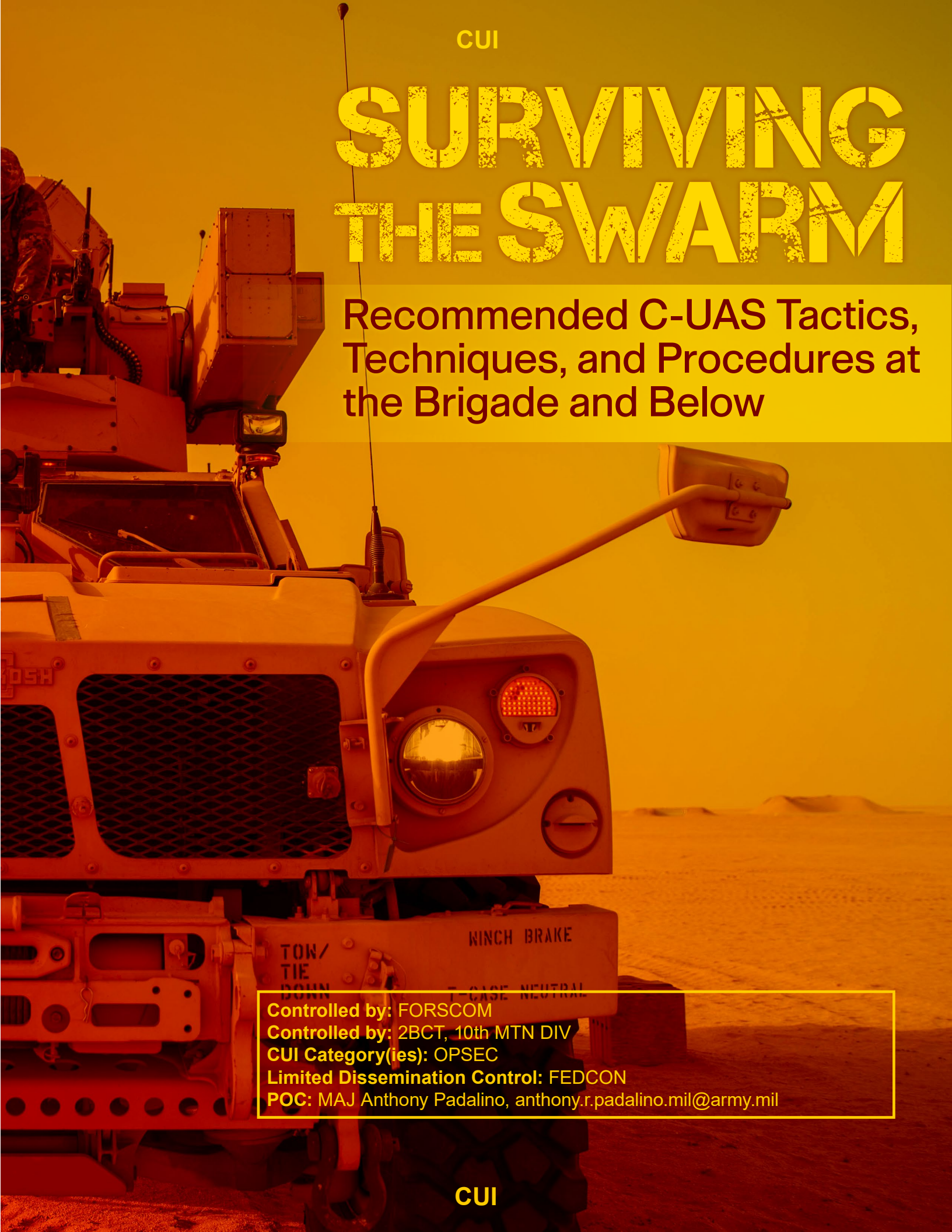
SURVIVING THE SWARM

Recommended C-UAS Tactics, Techniques, and Procedures at the Brigade and Below



Controlled by: FORSCOM
Controlled by: 2BCT, 10th MTN DIV
CUI Category(ies): OPSEC
Limited Dissemination Control: FEDCON
POC: MAJ Anthony Padalino, anthony.r.padalino.mil@army.mil

Center for Army Lessons Learned

The Center for Army Lessons Learned leads the Army Lessons Learned Program and delivers timely and relevant information to resolve gaps, enhance readiness, and inform modernization.

CONTACT US

10 Meade Ave.
Bldg 50
Fort Leavenworth
KS 66027

DSN: 552-9533
913-684-9533

DIRECTOR
COL Scott Allen

DEPUTY DIRECTOR
Rich Totleben

ANALYSTS/AUTHORS
Maj. Anthony Padalino
Gary Kuczynski

INFORMATION DIVISION CHIEF
Eric Hillner

CHIEF, PUBLISHING AND DIGITAL MEDIA
Diana Keeler

PUBLIC AFFAIRS OFFICER
Michael Hagen

EDITOR
Michaela Pursley

ILLUSTRATOR
Christie Blake

SECURITY
Sandra Griffin

WRITE with CALL

Have a game-changing best practice or compelling story? Let CALL lead you to publishing success!

We recognize your insights' immense value and potential impact. CALL offers unmatched resources and expertise to showcase your ideas in respected military journals.

Our team helps you easily shape your narrative and navigate the publishing journey. Don't let your knowledge go unnoticed—become a published author with CALL's support.

ARMY.MIL/CALL | (913) 684-9533/2255

TABLE OF CONTENTS

FIGURES

Introduction

In the contemporary operating environment, the U.S. Army is advancing its capabilities to effectively counter adversary unmanned aircraft systems (UASs). Acknowledging the need for improved counter-unmanned aircraft systems (C-UASs) tactics, techniques, and procedures (TTP) at the brigade level and below, this paper presents actionable solutions intended for immediate implementation. The 2nd Brigade Combat Team (BCT), 10th Mountain Division (2/10 MTN), deployed to the U.S. Central Command (USCENTCOM) area of responsibility from July 2023 to April 2024. The unit encountered more than 100 Iranian-made one-way unmanned aerial attack vehicles (OWUAS) targeting its positions in Iraq and Syria during their deployment. The leaders and Soldiers from 2/10 MTN gained unparalleled knowledge of C-UAS technical and tactical procedures while defending their bases from repetitive OWUAS attacks using the latest C-UAS technology and equipment. This paper extrapolates 2/10 MTN's C-UAS experiences within USCENTCOM and translates them into actionable lessons for U.S. Army brigade formations.

Chapter 1 enhances leader and Soldier familiarity with C-UAS doctrine for application in brigade C-UAS operations and offers recommendations regarding command and control (C2) systems and networks the U.S. Army uses for C-UAS operations. It also includes an overview of the C2 systems and networks the U.S. Army uses for C-UAS operations to enhance leader familiarity while providing future C2 network recommendations.

Chapter 2 details the C-UAS process integration for the brigade and below. It has a detailed analysis of the C-UAS process with recommendations to optimize brigade-level application in large-scale combat operations (LSCO) and defense of fixed sites. Chapter 2 also discusses operational focus areas, including the exploration of sensor employment, identification methods, and commonly used defeat systems to establish a viable C-UAS defensive plan. Finally, chapter 2 focuses on passive measures employment, including tactics on deploying decoys as a passive defense, enhancing the brigade's ability to conserve resources and deceive enemy targeting efforts.

Chapter 3 is a brigade C-UAS training guide. Senior leader training is a recommended executive course for consideration to educate senior leaders assuming base defense missions on equipment and processes overseen by their office. Chapter 3 includes a step-by-step C-UAS training outline for brigades, including active and passive C-UAS measures designed to escalate from individual skill development to the brigade culminating training event (CTE).

This paper seeks to convey the lessons learned from 2/10 MTN's front-line experiences and expert analysis, providing a solution for Army brigades to improve their C-UAS capabilities in LSCO and at fixed sites. By adhering to these recommended TTPs, Army brigades will meet the challenges of modern small, unmanned aircraft system (sUAS) threats with confidence and proficiency on the battlefield.

ADDITIONAL C-UAS READING

For more information on this topic at a higher classification, 2nd BCT and 2/10 MTN produced several C-UAS products, including white papers and instructional videos. They are available for units to review on the Center for Army Lessons Learned (CALL) SIPR website: https://dod365sec.spo.microsoft.scloud/teams/Army-TRADOC- CenterforArmyLessonsLearned/SitePages/C-UAS.aspx.

The Center for Army Lessons Learned (CALL) provides a unique service to the force by providing research and answers on a wide variety of topics.

CHAPTER 1

Overview of C-UAS Doctrine and Command and Control Systems

Note: Figures of equipment mentioned will not be displayed to prevent copyright infringement. However, links to websites will be provided to allow the reader to see the mentioned equipment and capabilities.

The contemporary operating environment is densely populated with commercial off-the-shelf (COTS) and military small, unmanned aircraft systems (sUAS), facilitating a broad spectrum of activities from intelligence, surveillance, target acquisition, and reconnaissance to physical and non-physical defeat capabilities.[1]

Reports highlight the continued use of unmanned aircraft systems (UAS) by the Houthi terrorists that have contested global trade routes with an effect not observed since the second World War. Iranian-aligned militia groups in Iraq and Syria routinely attack American bases with sUAS and one-way unmanned aerial attack vehicles (OWUAS).

The conflict in Ukraine exemplifies the relentless innovation and deployment of sUAS in large-scale combat, despite substantial losses, indicating a persistent trend toward the integration of unmanned systems in large-scale combat operations (LSCO). Ukraine and Russia have effectively used sUAS for intelligence, surveillance, target acquisition, and reconnaissance, as well as lethal strikes, leveraging COTS and military drones for tactical and strategic operations.[2]

Ukraine's adaptation of internationally procured and domestically produced sUAS for anti-armor and precision strikes highlights the adaptability of sUAS in modern conflict. Ukraine's success is paralleled by the Russian forces' goal of the proliferation of more than one million drones in 2024.[3]

Social media and open-source platforms reveal the diverse applications of sUASs, from disruptive tactics against key infrastructures to precision strikes on high-value military targets, underscoring their multifaceted role on the modern battlefield.[4] This evolving landscape of drone warfare demonstrates the need for adaptation and innovation in counter-unmanned aircraft system (C-UAS) tactics at the brigade level and below to address the challenges presented by adversarial use of sUAS on the modern battlefield.

DOCTRINAL FOUNDATIONS IN C-UAS

The U.S. Army delineates its defensive C-UAS operations into passive and active measures.[5] Passive measures include actions units undertake to decrease the likelihood of detection by sUAS and improving the likelihood of survival by mitigating the potential effects of an air attack, if detected. Active measures involve a process in which units and Soldiers detect, identify, decide, and defeat threat sUAS within their area of operations (AO). The speed and efficiency with which units conduct the C-UAS process will determine the units' effectiveness in denying or destroying threats in the AO. Chapter 2 of this paper examines active and passive measures in further detail.[6]

There are six essential air and missile defense (AMD) principles and seven tenets to apply and tailor to C-UAS tactics, techniques, and procedures (TTP) at the brigade level.[7]

Essential Air and Missile Defense Principles

These principles—mass, mix, mobility, integration, flexibility, and agility—are foundational in employing C-UAS assets effectively while ensuring a unified operational approach.[8] Adapting the six AMD principles to the brigade level involves a tailored approach that aligns with brigade-specific operational needs and capabilities. These principles, designed to enhance the effectiveness of C-UAS operations, ensure that brigades can employ a comprehensive tactical defense plan against sUAS threats.

The following explains how each principle should be applied within a brigade's operational planning:[9]

1. Mass: Focus on concentrating sufficient C-UAS firepower within the brigade to protect against sUAS surveillance or attacks. This will require prioritizing certain areas for defense while accepting risks elsewhere within the brigade's AO.

2. Mix: Use a diverse array of weapons and sensors at the brigade level to create a layered defense. This combination should offset the limitations of individual systems by exploiting the complementary capabilities of different technologies, thus enhancing overall protection.

3. Mobility: Ensure that C-UAS assets within the brigade are capable of rapid redeployment to support shifting operational dynamics and to maintain pace with maneuver elements. This mobility enhances the survivability of the defending units and the assets they protect.

4. Integration: Seamlessly integrate brigade C-UAS operations with adjacent brigade, division, and wider joint and combined air defense efforts. This integration should extend to coordinating the establishment of C-UAS positions along seams and unit boundaries, enabling the establishment of command and control (C2) networks with redundant capabilities for threat alert and target handoff.

5. Flexibility: Empower brigade commanders and their staff to apply C-UAS technical configurations and tactics to non-program of record and program of record systems in response to evolving threats and operational circumstances. This principle supports the ability to quickly adjust defensive postures as new intelligence and threat patterns emerge.

6. Agility: Cultivate the brigade's capacity to react swiftly to changing aerial threats, enabling a faster response than adversarial forces. Agility in AMD operations allow the brigade to preemptively counter or mitigate the effects of sUAS engagements.

Implementing these principles at the brigade level demands a pragmatic and adaptable approach, ensuring that C-UAS tactics are applied to the operational challenges and limited capabilities of brigade-sized elements and below. This tactical application of AMD principles enhances the brigade's ability to protect its forces and assets against a complex array of aerial threats.

AMD Employment Tenets

The AMD employment tenets provide tactical employment techniques of limited C-UAS systems. The AMD tenets (mutual support, weighted coverage, overlapping fires, early engagement, balanced fires, defense in depth, and resilience) ensure a robust defense posture, enabling forces to counter sUAS threats effectively through positioning limited resources (see Figure 1-1).[10]

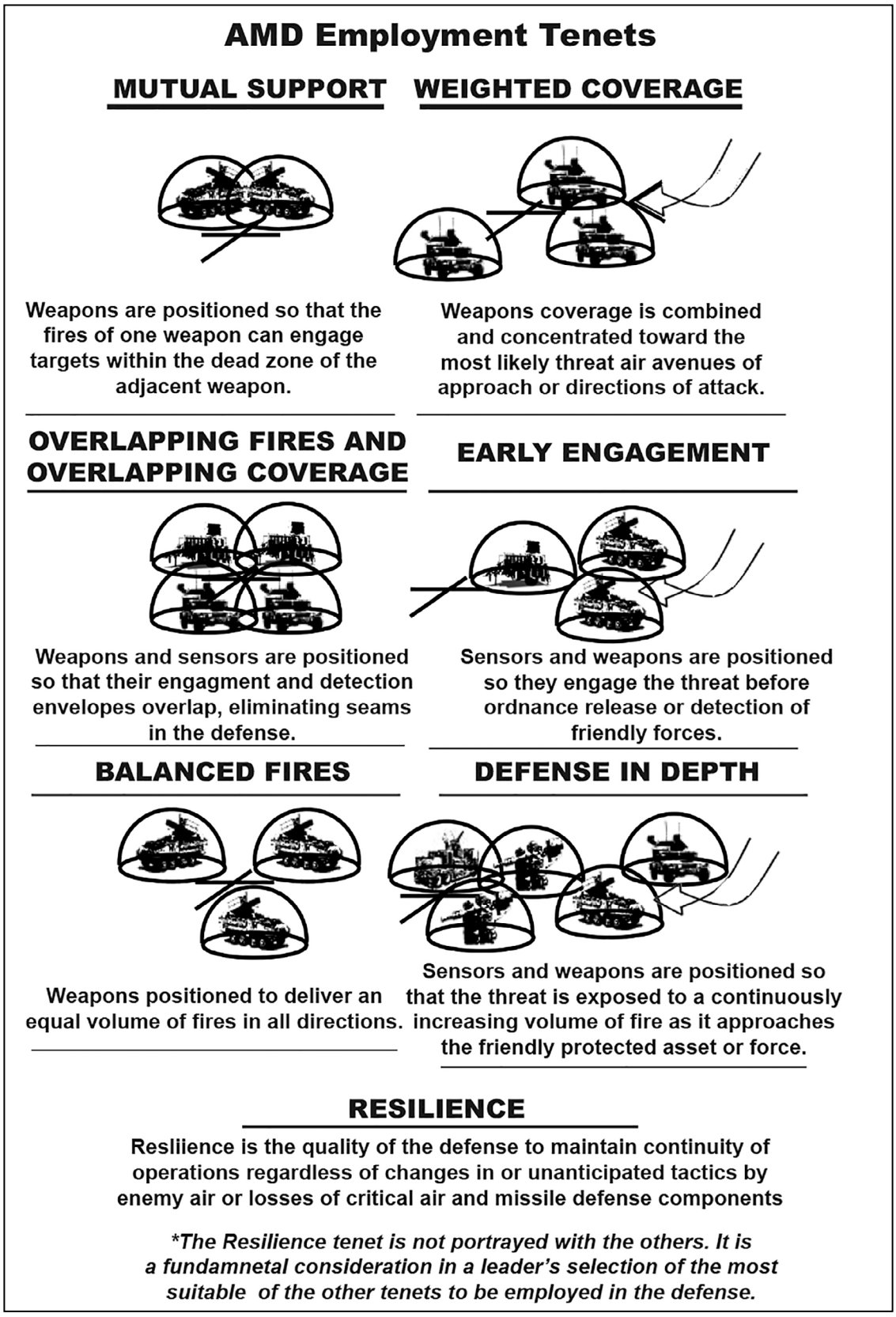


Figure 1-1. Air and missile defense tenets[11]

U.S. ARMY C-UAS C2 SYSTEMS AND NETWORKS

The U.S. Army's forward area air defense (FAAD) C2 system ties in active sensors and air defense defeat capabilities for the U.S. Army. The FAAD C2 operates on an internal inter-FAAD C2 network (IFN) and an external joint data network (JDN) that leverages data from other sensors operating on the JDN. The JDN integrates various air defense data across the joint force into one common operational picture (COP) and displays that information in real time via the FAAD C2.[12] A brigade's air defense airspace management (ADAM) cell operates the only authorized FAAD C2 in the brigade. However, any government Miltope computer[13] can perform the FAAD C2 function when loaded with FAAD C2 software.[14]

In addition to the JDN, which pulls data into the FAAD C2 common air picture for situational awareness and target hand-off, the FAAD C2 also operates on the IFN, which is a network that connects multiple FAAD C2 systems to create a unified air picture and enhance air and missile defense interoperability. This network allows the integration of air track data from various sources to provide a comprehensive view of the airspace, enabling collective short-range air defense (SHORAD) systems to conduct C-UAS and SHORAD missions effectively. By receiving air track data from multiple sources, the IFN creates a single, integrated air picture that includes local air information and the status of SHORAD weapons. This interconnected system facilitates faster decision making and improved situational awareness.[15]

Why this Matters: In LSCO, effective C-UAS deployment necessitates the seamless integration of passive and active sensors throughout the battlefield into a unified air picture. Brigades cannot continuously operate active sensors in the contemporary operating environment without risking destruction by enemy fire. In C-UAS engagements observed in U.S. Central Command (USCENTCOM)—from threat detection to neutralization or the threat reaching its target—events unfold within four minutes or less. Given this constrained period and limited decision-making space, the integration of IFN and JDN is crucial to defeat sUAS. These networks enable brigades to access radar data across a division's front, allowing a brigade to "see" live air tracks with active radar sensors, even when their own active sensors are offline, in transit, or have been destroyed.

BRIGADE C-UAS C2 AND NETWORK REQUIREMENTS

Divisions play a critical role in enabling brigade success by establishing an IFN that connects all the divisions' active and passive sensors into the FAAD C2 network. This integration feeds sensor data into all FAAD C2's operations within the division, displaying a real-time common air picture down to the brigade level. It is vital sensor information to incorporate into digital COPs, such as MAVEN,[16] Project Maven DSD Memo,[17] or android team awareness kit (ATAK)[18] to quickly alert units at echelon of imminent threats. At fixed sites, the IFN relies on a centralized server functioning as the primary data hub. However, during offensive and defensive maneuvers, it is impractical to swiftly move these network server nodes to new locations. Consequently, transitioning to a cloud-based data system becomes a crucial requirement to effectively implement an IFN in LSCO. This approach will enable more agile and responsive network capabilities essential for the dynamic nature of LSCO.

Brigades face the challenge of combining passive and active sensors within the COP, ensuring the rapid defeat of confirmed hostile sUAS. The network capacity for rapid data transmission raises concerns about the efficiency of a C-UAS layered defense at the brigade level and below. This paper advocates for network enhancements to foster a durable and effective C-UAS network capable of efficient targeting data exchange.

COMMAND AND CONTROL SYSTEM RECOMMENDATIONS

C2 of C-UAS execution across brigade echelons (down to the squad level) requires a clear COP. FAAD C2 is the centralized air defense network hub.[19] Deployment of the ATAK on mobile ad hoc networks (MANETs),[20] such as multi-purpose unit 5(MPU5s),[21] facilitates the creation of a mesh C2 network and a clear COP. This network supports the transfer of secure, though unclassified, data and capitalizes on commercial and military communication channels for effective information dissemination. Addressing gaps will strengthen C-UAS C2 and enhance the COP.

REQUIREMENTS TO CLOSE THE BRIGADE C-UAS C2 NETWORK GAP

The U.S. Army needs a network solution capable of integrating data from the ATAK, along with passive sensor data, into the FAAD C2 network for a comprehensive common air picture at the brigade and below. This data integration is critical for bridging the operational divide between frontline units and the U.S. Army's primary C-UAS network and C2 system. Achieving this requires the establishment of a two-way data flow from secure but unclassified networks[22] to the IFN or JDN. Such a connection not only allows passive sensors to instantaneously cue active sensors but also facilitates the straightforward incorporation of industry C-UAS systems into the C-UAS C2 network via secure but unclassified communication links. The paragraphs below briefly describe the ATAK and MPU5.

Android Team Awareness Kit

The ATAK is the C2 system of choice used to create a COP that is designed for versatility at the brigade and below. ATAK plugin operates on electronic tablets and smartphones, integrating advanced features, such as real-time mapping, visual data sharing, and secure but unclassified encrypted communications. ATAK allows users to monitor team member locations, exchange photos and videos, and engage in effective collaboration across a spectrum of operational scenarios. ATAK has a customizable plugin architecture, which empowers developers to extend its capabilities with mission-specific functionalities.

MPU5 Smart Radio with Wave Relay Operating System

The MPU5 wave relay MANET is a C2 network requirement at the brigade and below used to seamlessly connect communication mediums, including upper and lower T/I, creating a direct communication link to the end user. It is the preferred device for integrating with ATAK plugin software because of its versatile capabilities. The MPU5 can handle voice, data, and high-resolution video transmissions, offering a robust communications infrastructure. This infrastructure supports multiple data transmission pathways within a unit's primary, alternate, contingency, and emergency (PACE) plan.

As a mesh-network device, the MPU5's effectiveness is maximized when deployed extensively across the brigade combat team (BCT). For an infantry brigade combat team (IBCT), equipping 450 MPU5 units (installed in vehicles, command posts, and carried by selected Soldiers) ensures the creation of a durable network. This network is adept at relaying data across different mediums using a single system, thus enhancing operational resilience.

C2 Network Importance

Understanding how C2 networks enable the C-UAS process enhances a unit's capability to leverage sensors and defeat capabilities to neutralize sUAS threats. Not all C-UAS systems will be present on the FAAD C2 network – this fact underscores the "systems-of systems" concept for C-UAS. For instance, a Soldier operating a FIM-92 Stinger[23] is directed to fire through the C-UAS process based on engagement criteria, not the FAAD C2 network. This example exemplifies how the speed at which a unit detects and disseminates information on the sUAS throughout the force determines an organization's ability to survive the swarm.

At fixed sites, such as in the USCENTCOM area of responsibility (AOR),[24] air raid sirens and loudspeakers alert forces to seek shelter, while alerting defenders to prepare their systems for intercept. However, in combat situations, a brigade must conduct C-UAS on the offense or defense, without the capability of a centralized C-UAS defense system. Given the presence of friendly manned and unmanned aircraft—including newly deployed RQ-28s,[25] friendly loitering munitions, and COTS first-person view drones—it is essential for brigades to have a C2 system and a robust network. This system should enable operators to identify targets quickly and accurately for physical action. Additionally, it must rapidly alert adjacent, subordinate, and higher headquarters, so they too can conduct their C-UAS process as a part of a C-UAS layered defense.

End Notes

1. Kunertová, Dominika, Contemporary Security Policy 44, no. 4 (2023): 576-591, *Drones Have Boots: Learning from Russia's War in Ukraine*, 4 October 2023, https://www.tandfonline.com/doi/pdf/10.1080/13523260.2023.2262792.

2. Schmidt, Eric, Foreign Affairs, *Ukraine Is Losing the Drone War: How Kyiv Can Close the Innovation Gap With Russia, Foreign Affairs*, 22 January 2024, https://www.foreignaffairs.com/ukraine/ukraine-losing-drone-war-eric-schmidt.

3. Ibid.

4. COL Antal, John F., Havertown: Casemate Publishers, *Next War: Reimagining How We Fight*, 28 September 2023.

5. Army Techniques Publication (ATP) 3-01.81, *Counter-Unmanned Aircraft System (C-UAS)*, 11 August 2023.

6. Ibid.

7. Field Manual (FM) 3-01, *U.S. Army Air and Missile Defense Operations*, 22 December 2020.

8. Center for Army Lessons Learned (CALL), *Commander and Staff Guide to Counter-Small Unmanned Aircraft Systems in Large-Scale Combat Operations*, 2022, https://call2.army.mil/toc.aspx?document=18223.

(CAC login required)

9. FM 3-01, *U.S. Army Air and Missile Defense Operations*, 22 December 2020.

10. CALL No. 18-16, Maneuver Leader's Guide to Stinger, April 2018, https://usacac.army.mil/node/2013.

11. CALL No. 22-07, *Commander and Staff Guide to Counter-small Unmanned Aircraft Systems (C-sUAS) in Large-Scale Combat Operations (LSCO)*, September 2022, https://armyeitaas.sharepoint-mil.us/teams/lessonslearned/CALL%20Publications/Forms/AllItems.aspx?id=%2Fteams%2Flessonslearned%2FCALL%20Publications%2F22%2D07%20%28650%29%5FcUAS%20during%20Div%20and%20Corps%20LSCO%20%28Sep%2022%29%20%28CUI%29%2Epdf&parent=%2Fteams%2Flessonslearned%2FCALL%20Publications.

(CAC login required)

12. Ibid.

13. According to their website, Miltope is the leading manufacturer of rugged computer, server/mass storage and network peripheral equipment solutions for military, industrial, and commercial aviation applications that call for reliable performance under demanding environmental conditions. The U.S. Army uses the following equipment: RLC-4G Rugged Laptop Computer | Miltope (mymiltope.com).

14. According to their website, Northrop Grumman's short-range air defense (SHORAD) capabilities protect U.S. and allied forces from a wide range of manned and unmanned air and missile threats. Their capabilities integrate sensors, weapons, and C2 to acquire, track, verify, engage, and defeat current and evolving threats. Northrop Grumman is leveraging its work on Initial Maneuver-Short Range Air Defense IM-SHORAD to advance the Army's shift to great-power focused, multi-domain operations, specifically for the maneuver short range air defense mission. FAAD C2 can be found at Short-Range Air Defense (SHORAD) | Northrop Grumman.

15. Northrop Grumman, *Northrop Grumman's FAAD C2 System Enables Integrated Short Range Air Defense in Baltic Region*, 2023, https://news.northropgrumman.com/file/northrop-grummans-faad-c2-system-enables-integrated-short-range-air-defense-in-baltic-region?action=.

16. Choudhury, Rizwan, Interesting Engineering, *Project Maven: The epicenter of US' AI military efforts*, 2 March 2024, https://interestingengineering.com/military/project-maven-the-epicenter-of-us-ai-military-efforts.

17. Deputy Secretary of Defense, *Memorandum*, 26 April 2017, https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%20020170425.pdf.

18. TAK.gov. Military. Retrieved 20 May 2024, https://tak.gov/solutions/military.

19. FM 3-01, *U.S. Army Air and Missile Defense Operations*, 22 December 2020.

20. Defense Advancement, Using MANET for Reliable Ad Hoc Networking, 30 November 2022, https://www.defenseadvancement.com/news/using-manet-for-reliable-ad-hoc-networking/.

21. According to their website, the MPU5 is the world's first smart radio with an onboard wave relay operating system that includes everything needed built in. Retrieved 20 May 2024, https://www.persistentsystems.com/mpu5-capabilities/.

22. Maj. Blumberg, Matthew S., Military Review, *The Integrated Tactical Network: Pivoting Back to Communications Superiority*, May-June 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2020/Blumberg-Int-Tactical-Network/.

23. According to this site, the FIM-92 Stinger is a man-portable surface-to-air missile system that was designed and manufactured by the American defense industry. The Stinger was the successor to the Redeye Weapon System. The Stinger missile provides forward, short-range air defense against low-altitude airborne targets. The United States and 29 other countries use the system. It is manufactured by Raytheon Missile Systems and under license by EADS in Germany. The Stinger Weapon System provides superior air defense for today's highly mobile forces. Stinger has been combat-proven in four major conflicts and has more than 270 fixed-wing and rotary-wing kills to its credit. Stinger-RMP is a lightweight, self-contained air defense system that can be rapidly deployed on military platforms in any combat situation. Stinger-RMP (Reprogrammable Microprocessor) missiles are used interchangeably, on helicopters for air-to-air self-defense teams for surface-to-air engagements. Immediately after launch, the gunner is free to take cover to engage additional targets, thereby maximizing survivability and combat effectiveness. Global Defense News, *Man-portable surface-to-air defense missile system – United States*, 12 July 2024, https://www.armyrecognition.com/military-products/army/air-defense-systems/man-portable-air-defense-systems/stinger-fim-92-united-states-uk.

24. U.S. Central Command, https://www.centcom.mil/AREA-OF-RESPONSIBILITY/.

25. Hylton, David, U.S. Army, *New short range reconnaissance capability begins fielding to Soldiers*, 12 October 2022, https://www.army.mil/article/261063/new_short_range_reconnaissance_capability_begins_fielding_to_soldiers.

CHAPTER 2

C-UAS Process Integration for the Brigade and Below

The U.S. Army counter-unmanned aircraft systems (C-UAS) process—detect, identify, decide, defeat—provides a framework to examine the C-UAS systems-of-systems approach at echelon (Figure 2-1). Having a basic understanding of the various command and control (C2) systems and networks is vital to achieving a layered defense against small, unmanned aircraft systems (sUASs) across the brigade. An efficient C-UAS process enables an infantry squad that detects a group 1-3 sUAS[1] to pass the air track data through the company, battalion, and brigade echelons within 60 seconds or less.

It is difficult to achieve efficiency in the process even when defending fixed site locations, such as those in U.S. Central Command (USCENTCOM), where active and passive sensors continually cue without threat of destruction by a peer adversary and the base defense operations center (BDOC) controls all intercept options. In a distributed large-scale combat operations (LSCO) environment, brigades will have the task of achieving a layered defense over dispersed C2 nodes, making the process even more difficult.

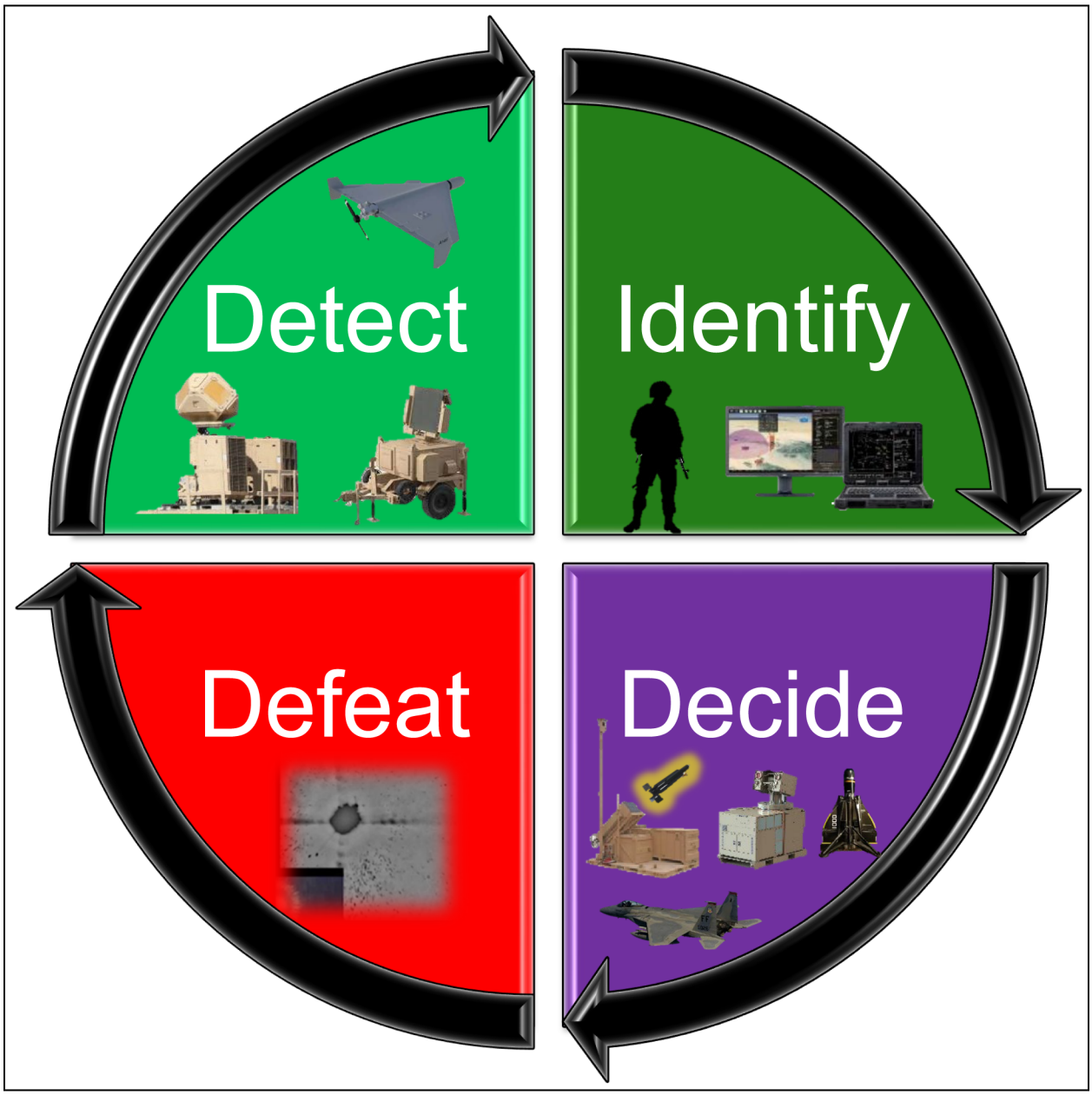


Figure 2-1. Counter-unmanned aircraft system process[2]

Within the C-UAS layered defense system, each echelon, from the fire team to the brigade main command post, executes the C-UAS process with the equipment at their disposal. At the squad level, Soldiers will first detect, identify, decide, and defeat identified threat sUAS, while alerting others in their area of operations (AO) through the robust C2 network. Should one layer fail to neutralize the threat, subsequent layers at the platoon, company, or battalion level continue to engage until they eliminate the threat, or the threat strikes its objective. The success of C-UAS layered defense in LSCO hinges on the C2 network's ability to rapidly relay data across echelons.

U.S. Army C-UAS engagements typically conclude in less than four minutes during combat operations within the USCENTCOM area of responsibility (AOR). This means Soldiers have less than 60 seconds to make an intercept decision after detecting a potential threat.

DETECT

The detection phase is foundational in the C-UAS process. It aims to detect the presence of sUAS within the operational area, emphasizing detection rather than immediate hostile identification—this differentiation occurs in the subsequent phase. Before launch of C-UAS, the detection of sUAS in the AO must occur, giving early warning to the active defeat process.

Effective intelligence collection that spans the depth of the operational area, harnessing real-time signals intelligence to locate sUAS operators, crafts, or their control stations will enable sUAS interdiction "left of launch" (before launch). This comprehensive approach is necessary not only across the forward line of own troops (FLOT) but also in rear and close areas. The aim is to pinpoint sUAS launch/recovery sites and ground control stations, which are integral to the sUAS threat landscape. Brigade and battalion plans should include these elements in their battlefield intelligence preparation and target nominations, considering the unique electromagnetic signatures of sUAS communications and control links.

After a threat launches an sUAS, active detection occurs using passive and active sensors. This phase identifies low, slow, and small UAS. The U.S. Army, joint force, and industry partners have a variety of sensors to assist with the detection phase. However, it is critical for leaders to understand that the radars' max range capabilities do not detect ranges for group 1-3 sUAS. Factors, such as the radar's location, the sUAS's size, radar cross section, and its flying altitude in restrictive terrain can significantly reduce radar detection capabilities. For effective detection planning, units should conservatively estimate that sUAS detection will happen at approximately 50 percent of the maximum range of a system. This assumption is crucial for planning as delayed detection reduces the time available to counter the threat.

Lethal defeat systems, which neutralize threats through physical means, typically rely on a fire control radar (FCR) to lock onto and engage the target. It is crucial leaders know and understand which systems rely on an FCR to conduct an engagement, which will be a consideration in its protection prioritization and cueing schedule. Brigades operating in an LSCO environment that are equipped with a C-UAS lethal defeat reliant on a single FCR should only activate the FCR outside enemy strike range or when cued by passive radar or another intelligence source. This tactic is essential to protect the survivability of the C-UAS lethal defeat systems.

Detection Systems Overview

Raytheon's AN/MPQ-64 Sentinel Radars[3] and Lockheed Martin's Q-53 Multi-Mission Radars.[4] The U.S. Army Division Artillery (DIVARTY) is equipped with Raytheon's AN/MPQ-64 Sentinel Radars and Lockheed Martin's Q-53 Multi-Mission Radars. These radars offer comprehensive, 360-degree detection of air and missile defense (AMD), UAS, and rotary and fixed-wing aircraft. These systems are calibrated to identify low, slow, and small UAS; execute identification, friend or foe (IFF) procedures; and relay detections through the JDN and integrated fire network (IFN) to subordinate brigade's forward area air defense (FAAD) C2. The effectiveness of the Q-64 in performing IFF is contingent on its ability to detect aircraft. The battlefield layout and the radars' proximity to the front lines influences this task.

Brigades are equipped with Lockheed Martin Q-53 radars, capable of operating in 360-degree and focused 90-degree modes. Brigade Q-53 radars do not include the Multi-Mission Radar hardware and software upgrades necessary for IFF capabilities (the ability to decode aircraft modes and codes). Nevertheless, brigades can enhance their Q-53 radars with a "Multi-Mission Radar-Lite" software update, affording them the capacity to track air movements without full IFF functionality.[5]

Raytheon's Ku-Band Radio Frequency System (KuRFS).[6] Raytheon's KuRFS represents a pivotal 360-degree active sensor within the low, slow, small, unmanned aircraft integrated defeat system (LIDS). KuRFS not only contributes to counter-rocket, artillery, and mortar efforts but also supports the Raytheon Coyote interceptor. Directly integrated into the FAAD C2 system, KuRFS serves as the FCR for the land-based Phalanx Weapon System and the Coyote interceptor, streamlining target acquisition and engagement processes.

Brigade C-UAS Sensor Employment

Brigades should array passive and active sensors across their formations, as outlined in Figure 2-2. Active sensors, because of their electromagnetic emissions, are easily detected by adversaries and therefore must be highly mobile. They should operate under strict cueing protocols and schedules to minimize detection risks. Passive sensors, including acoustic and radio frequency (RF) sensors, play a crucial role in early threat detection, cueing defeat mechanisms, and alerting Soldiers to imminent dangers.

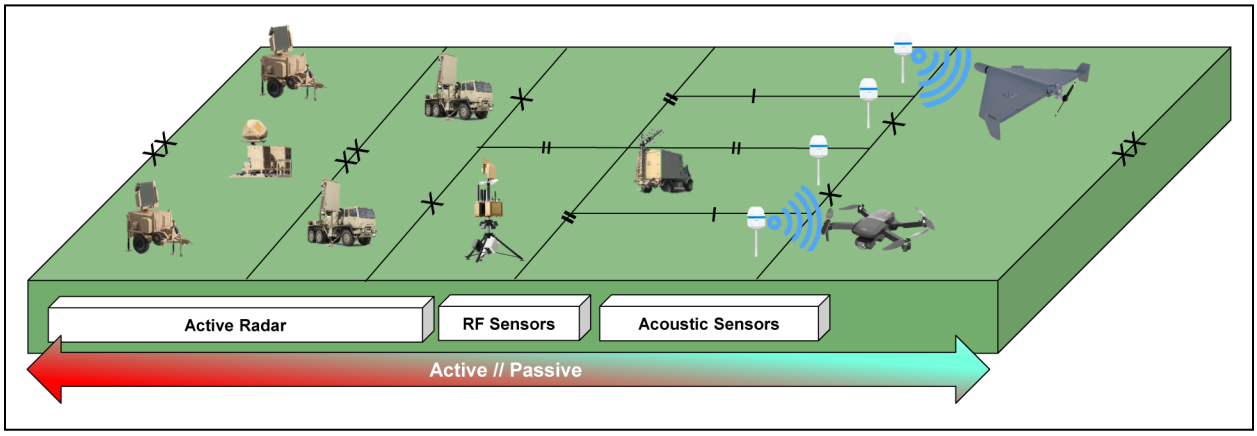


Figure 2-2. Brigade C-UAS sensor employment sketch[7]

There is an operational intersection between active radar systems and passive RF and acoustic sensors. This integration is essential for certain lethal defeat systems that depend on active radar for FCR functionality. The brigade's primary challenge during the detection phase lies in the real-time ingestion and dissemination of sensor data into the common operational picture (COP). Achieving this allows effective cueing of active radars and timely alerts to formations upon the detection of threat sUAS. Bridging this gap ensures a cohesive response mechanism, leveraging passive and active sensor capabilities to maintain situational awareness and enhance defensive postures against UAS threats.

IDENTIFY

Timely and accurate identification during C-UAS operations is critical. It involves rapidly analyzing detected contacts to determine whether they are friendly, neutral, or hostile. The goal is to identify these contacts as early as possible to maximize the window for engagement and minimize the risk of fratricide. Given the complexity of modern battlefields, where friendly and adversary forces operate the same groups of UAS, precise identification is crucial. Identification enables leaders to move to the next phase in the C-UAS process and make informed engagement decisions. With their enhanced situational awareness, leaders can optimize weapon deployment, conserve friendly resources, and reduce friendly fire incidents.

Methods of Identification

Two primary methods are employed for the identification of contacts and are discussed below:

1. Procedural Identification: This method categorizes airspace users based on their location, altitude, heading, time, and flight patterns. It relies on predetermined rules and patterns of movement to separate friend from foe. For example, any sUAS flying outside established air corridors at a certain time could be procedurally identified as hostile.

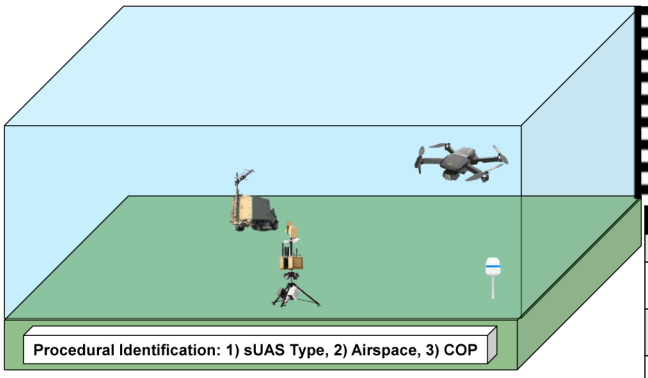
2. Positive Identification: This is the preferred method of identification and involves the direct observation and analysis of target characteristics. It could include visual confirmation, the use of electronic support systems, non-cooperative target recognition techniques, and IFF systems. Positive identification seeks to conclusively determine the nature of the target through its observable characteristics and behaviors.

Typically, units use a combination of procedural and positive identification methods during operations to ensure accuracy. Positive identification allows the categorization of a UAS by specific name, category, or exact make and model, and, when possible, the identification of its payload. This detailed level of identification is vital for choosing the appropriate response and engagement method.

Early and accurate identification of sUAS is an instrumental part of the C-UAS process. It extends the available time for engagement decisions, enhancing the effectiveness of responses while preserving the safety of friendly forces. Timely identification allows a broader range of weapons employment options, ensuring the efficient use of resources while minimizing the risk of engaging friendly or neutral UAS. The complexity of the task cannot be overstated, as the operational environment often features UAS that are identical in appearance but differ in allegiance.

Brigade and Below C-UAS Identification

Within the brigade, every echelon uses procedural and positive identification methods to identify sUAS as friendly or hostile. At the company and battalion levels, positive identification often relies on forward air guards positioned at listening posts/observation posts equipped with acoustic and RF sensors, or through thermal and full-motion video systems deployed within the operational area. Procedural identification comes into play when sUAS detected by passive sensors are cross-referenced with the COP specific to the unit's AO (Figure 2-3). At this stage, company-level leaders apply their insight into enemy capabilities and the situational context to their digital COP to procedurally classify an sUAS as hostile, advancing to the subsequent phase of the C-UAS process.



Example Procedural Identification Criteria		
IF	**AND**	**THEN**
Acoustic Sensor Alerts sUAS outside of AO	No Friendly sUAS on ATAK COP	PID Hostile
Acoustic Sensor Alerts sUAS	Friendly sUAS in adjacent AO	PID Suspect
RF Sensor Alerts sUAS	RF Freq not on friendly band	PID Hostile
Acoustic/RF Sensor Alerts sUAS within/vectoring to AO	No friendly sUAS on ATAK COP	PID Hostile
Acoustic Sensor Alerts sUAS within of AO	Friendly sUAS on ATAK COP	PID Friendly

Figure 2-3. Procedural identification example[8]

It is crucial to conduct the identification process at the most decentralized leadership level feasible to facilitate swift action by defeat systems before the threat sUAS can execute an attack on the formations. Training in accurate procedural identification of threat sUAS is essential because of the frequent operation of friendly sUAS in proximity to forward troops as part of intelligence gathering and battlefield shaping operations at the brigade, division, and corps levels.

Commanders must implement engagement criteria and establish straightforward procedural control measures that support quick decision making at the lowest levels. For instance, consider an sUAS operating below 3,000 feet above ground level (AGL) within a platoon's AO. Given specific identification criteria provided below, a junior Soldier can procedurally classify this sUAS as a threat and proceed accordingly in the next phase of the C-UAS process.

At the brigade level, radars tasked with detecting sUAS project their findings onto the FAAD C2 common air picture. When a radar equipped with IFF capabilities detects a track, the operator can interrogate the track for specific modes and codes to ascertain its status. However, in instances where a radar lacks IFF capabilities, such as the KuRFS, the FAAD C2 operators must analyze the track's physical characteristics to assess whether it represents a friendly or hostile entity. This approach constitutes procedural identification at the brigade main command post.

FAAD C2 operators employ a methodology known as BARS (bearing, altitude, range, and speed) to perform procedural identification in the absence of IFF data. This method involves analyzing the trajectory, altitude, distance, and velocity of the detected craft to make informed judgments about its nature. For example, a brigade can procedurally classify as hostile an aircraft moving toward or already within the brigade's AO at an altitude and speed inconsistent with those of brigade-deployed sUAS, or not adhering to pre-established air corridors as outlined in the brigade's airspace management plan. This determination allows operators to advance to the decision-making phase, in which they employ physical or non-physical systems against an identified threat.

Understanding the steps and procedures to rapidly identify an air track friend or foe is vital. When training the C-UAS process, units must highlight the reliance on technological and analytical methods to ensure airspace security in the absence of direct identification capabilities. This enables the brigade units to maintain a defensive posture against potential sUAS threats.

Figure 2-4 outlines a FAAD C2 located at the brigade main command post, identifying an sUAS as hostile within the brigade AO. After marking this track hostile, it populates on all FAAD C2s throughout the joint force via IFN and JDN networks. Brigades must alert subordinate battalions of the threat's position, enabling subordinates to attempt to intercept the threat, disperse congested formations, or displace critical enablers.

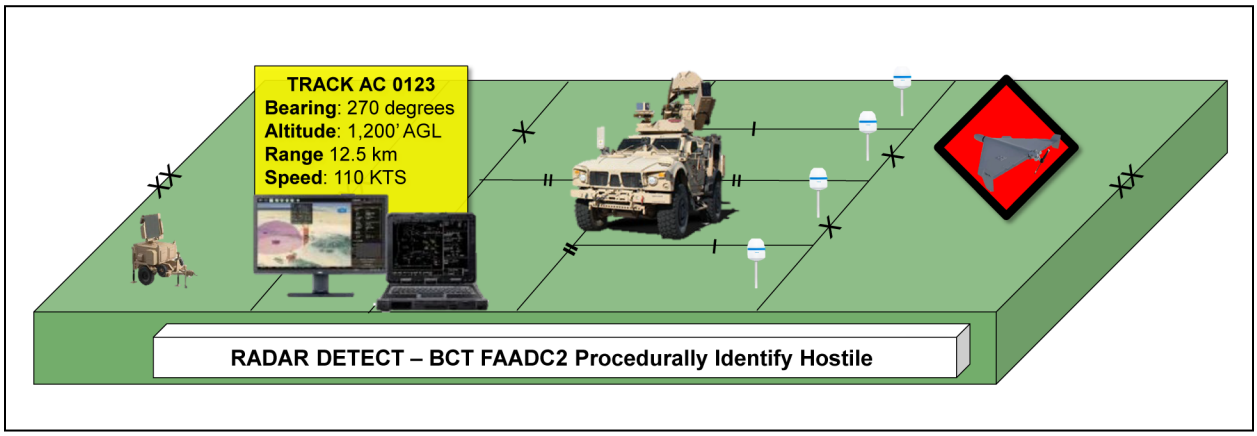


Figure 2-4. Brigade air defense and airspace management cell procedurally identifies hostile sUAS[9]

DECIDE

There are two critical considerations in the decide phase, as follows:

1. Determine the necessity to engage a detected UAS
2. Select the appropriate methods to mitigate or eliminate the identified threat[10]

This phase includes physical and non-physical approaches, with some electronic warfare (EW) capabilities that span both categories. The rules of engagement guide the decision-making process, the tactical necessity of intercept, and the inherent right of self-defense. The engagement process will vary based on defending from a fixed site or from a maneuvering location. The selection of a defeat system to counteract an sUAS threat is dependent on the quantity and classification of the sUAS (ranging from groups 1 to 3) and the nature of the defense location—whether it is a static fixed site or a mobile maneuvering brigade.

For example, operators at a fixed site of strategic or operational significance might deploy a full spectrum of systems to neutralize a threat, prioritizing the mitigation of potential damage over the cost of munitions used. Conversely, a maneuvering brigade, lacking the same level of defense in depth, may opt for a more selective application of interceptive measures. The brigade might decide against employing certain counter-sUAS technologies for a specific threat, particularly if the sUAS is not targeting a high-priority area as determined by the commander. This approach reflects the battlefield calculus of balancing resource expenditure against the imperative to protect critical assets, adjusting the response to the sUAS threat based on the operational context and the assets at risk.

Fixed Site C-UAS Defense

The BDOC plays a pivotal role in C-UAS operations at fixed sites. A "BDOC is a C2 facility established by the base commander to serve as the primary center for force protection, security, and defense within the base boundary."[11] A BDOC relies on standoff distances provided by a base defense zone,[12] which is a designated block of airspace and ground area extending to a specific range from the base's perimeter. The base defense zone (shown in Figure 2-5) is within the defending unit's BDOC AO, and within it, the BDOC holds target engagement authority over all aircraft that enter. Upon detection and identification of a threat within the base defense zone, the unit engages the sUAS within the C-UAS process, facing the base's layered defense system until the threat is either neutralized or achieves its mission objective.

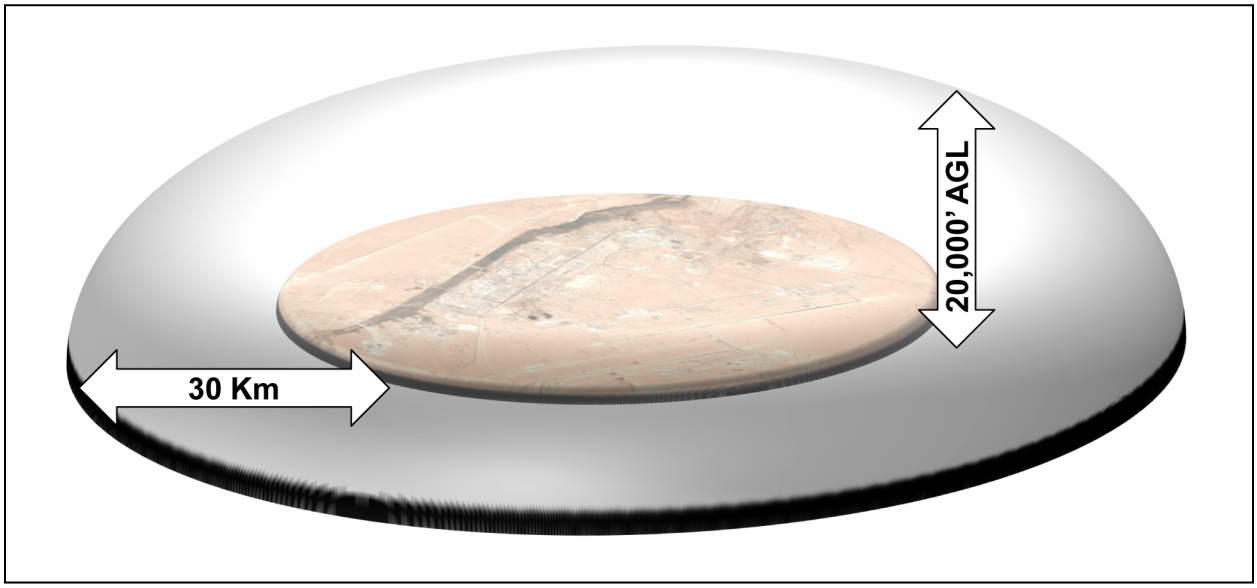


Figure 2-5. Base defense zone[13]

The concept of fixed site layered defense initiates from the center, often referred to as the "bullseye," which represents the core of the defended location. At this nucleus, C-UAS operators employ a comprehensive array of systems to intercept and counteract the identified threat, effectively orchestrating a defense-in-depth strategy to safeguard the base. BDOC officers in charge (OIC) and noncommissioned officers in charge (NCOIC) are the release authority for all actions within the base defense zone. Lieutenants and staff sergeants orchestrate and execute the C-UAS process. In the decide phase, the BDOC will determine the likely size of the craft based on BARS and will typically engage group 2+ threats before obtaining visual identification with full motion video. The decision on defeat employment system depends on the threat classification type, the systems on hand, and weapons ranges.

Figure 2-6 provides an illustration of an identified hostile group 3 sUAS vectoring to a fixed site location. The weapon system with the most standoff range is the first to prosecute the threat sUAS. This could be defensive counterair (DCA) platforms, either from manned or unmanned systems flying combat air patrols (CAP); or ground-based interceptors, such as the Raytheon Coyote or the Anduril Road Runner.

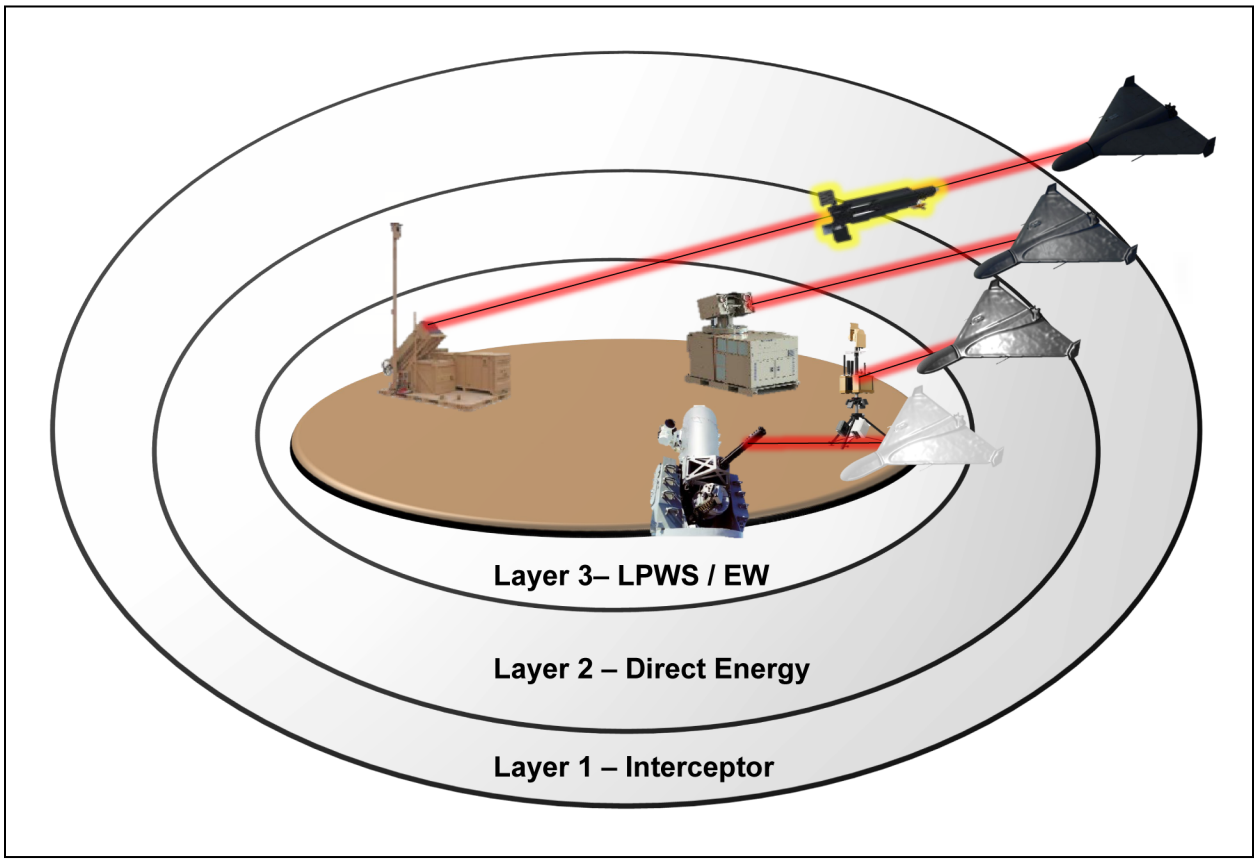


Figure 2-6. Fixed site layered defense[14]

If these systems fail to intercept the threat or the amount of threat sUAS outnumbers the interceptors available, the BDOC will activate the next layer by engaging with subsequent physical and non-physical systems, such as Stinger missiles, direct energy laser, microwave weapons, EW systems, land-based Phalanx Weapon Systems, or individual direct fire weapons.

Brigade C-UAS in the Offense and Defense

The approach to layered defense and the C-UAS process undergoes significant adaptation when units transition from static defense at fixed sites to dynamic offensive and defensive operations. Unlike the centralized detection and defeat mechanisms coordinated through a BDOC in fixed-site scenarios, units on the move—particularly brigades—must decentralize these capabilities. Despite retaining most active sensors and lethal systems, the expansive nature of the AO compels brigades to implement C-UAS defensive tactics, such as mutual support, overlapping coverage, and balanced protection, as previously outlined in the tenets of AMD (Figure 2-7).

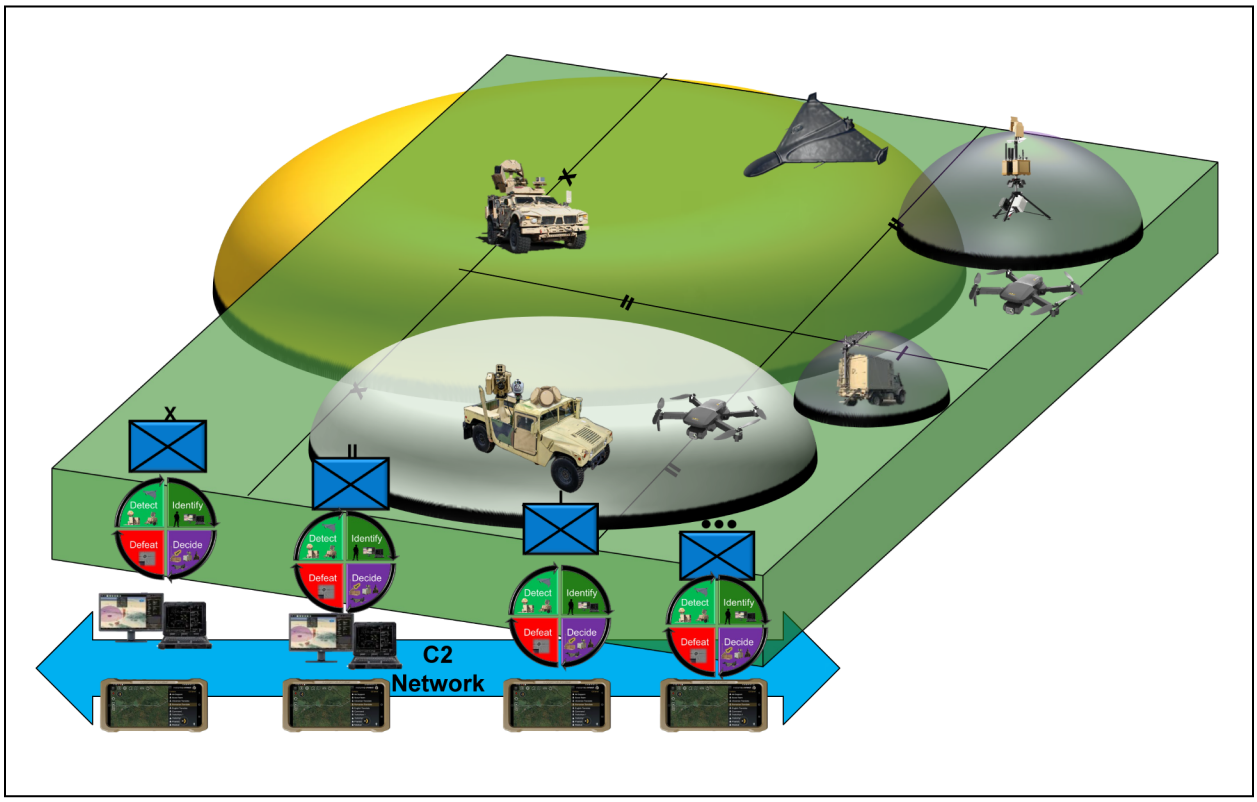


Figure 2-7. Brigade C-UAS overlapping defensive fires[15]

The decision-making process regarding protection priorities and engagement criteria at each echelon is critical to dynamic defense. Not all detected sUAS warrant engagement with ground-based or aerial interceptors. For instance, the detection of a Group 1 sUAS quadcopter identified beyond the FLOT within the brigade's AO by EW assets presents a tactical decision point. At the platoon and company level, leaders may opt to defeat the system with their equipment to achieve their mission, whereas the battalion and brigade echelons may monitor the threat but choose not to engage the threat with lethal capabilities. Even if the battalion's or brigade's active radar confirmation of the sUAS presence occurs, the absence of non-lethal engagement options necessitates a calculated response. Deploying valuable interceptors, such as the Raytheon Coyote or Anduril Road Runner, against such a minimal threat may be a misallocation of resources better reserved for neutralizing more substantial sUAS threats, including loitering munitions.

Maintaining discipline in adherence to established defensive fires engagement criteria is crucial. This discipline ensures that brigades judiciously use their limited assets, prioritizing the engagement of threats that pose the most significant risk to their mission. Such vital resource management is crucial to maintain an effective and sustainable C-UAS defense posture during mobile operations, in which the fluidity of the battlefield and the volume of threats can quickly deplete defensive resources if not managed with precision and foresight.

Physical Methods of Engagement

Physical engagement involves direct interaction with the UAS to render it inoperative. Methods include the use of drone interceptors; small arms; projectiles; directed energy weapons, like lasers and high-power microwaves; and entanglement techniques like nets. Specifically, small arms defense techniques emphasize volume fire and proper aiming to counter low-flying UAS threats. The effectiveness of small arms is confined by the weapon's range and destructive capacity, making them suitable primarily for engagements with low-altitude UAS.[16]

The brigade's decision to employ small arms against UAS threats rests with unit commanders and hinges on an evaluation of the severity of the threat against the potential drawbacks on unit effectiveness. The engagement area's characteristics (urban versus rural, etc.) and the ability to apply a volume fire to possibly deter or disrupt the UAS pilot's course of action will inform this decision. Units use the football field technique to estimate lead distance for aiming, promoting a uniform response among Soldiers, and maximizing the effectiveness of massed fire.

Non-Physical Methods of Engagement

Non-physical methods of engagement focus on disrupting or commandeering the UAS's communication and control mechanisms without direct physical interaction. These techniques may still inadvertently lead to the UAS's crash, potentially causing collateral damage. Examples include radio frequency jamming; GPS jamming and spoofing; dazzling; and jamming of position, navigation, and timing signals.[17] These methods are integral to a comprehensive C-UAS strategy, offering alternatives when physical engagement is impractical or could result in unintended consequences. An example of this non-physical method is the Dronebuster EW system, found at Flex Force Enterprises.[18]

In summary, the decide phase is a multifaceted process requiring commanders to assess the necessity and means of engaging a UAS threat quickly and methodically. This decision is critical for maintaining operational security and effectiveness. It involves a balanced consideration of physical and non-physical tactics to mitigate the risks posed by unmanned threats in the battlefield environment. This comprehensive approach ensures that commanders have the flexibility and tools necessary to protect their units and accomplish their missions within the constraints of operational directives and the realities of modern aerial warfare.

DEFEAT

The defeat phase culminates the C-UAS process, in which operators employ selected means to neutralize identified threats. Units confirm their success in this phase through visual or digital means. This phase underscores the importance of persistence and adaptability in defense operations, ensuring threats do not reach their intended targets.

There are hundreds of systems in the C-UAS industry. In 2023, there were more than 290 commercial companies with C-UAS solutions listed in the *2023 C-UAS Buyers Guide*. In the section below, there is an overview of a few common defeat systems in use by the Department of Defense (DOD) and U.S. Army.

Common DOD Defeat Systems

LIDS: low, slow, small, unmanned aircraft integrated defeat system. The U.S. Army's C-UAS LIDS is a comprehensive C-UAS system to effectively detect and defeat UASs. Key components of the LIDS system include Raytheon's KuRFS radar and Coyote effector, which work together to detect, track, identify, and defeat Group 1-3 UAS threats. The system is deployable in mobile and fixed configurations, offering flexibility in deployment scenarios. Additionally, LIDS incorporates Northrop Grumman's FAAD C2 and EW systems for a robust C-UAS solution.[19]

Anduril Roadrunner. The Anduril Roadrunner is a vertical take-off and landing autonomous air vehicle designed for efficient C-UAS operations. It combines recoverable lethal strike capabilities with the agility and speed needed to swiftly identify, intercept, and neutralize aerial threats. Characterized by its high subsonic speeds, exceptional maneuverability, and fast response times, the Roadrunner bridges the cost and capability gap between smaller UAS and larger aircraft. Its dual jet propulsion, modular payloads, and quick turnaround for refueling enhance adaptability and readiness against a variety of threats. The enhanced Roadrunner-M variant further improves ground-based air defenses with quicker launches, greater payload capacity, and extended range, outperforming similar systems in maneuverability.[20]

MSI EAGLS. The MSI electronic advanced ground launcher system (EAGLS) C-UAS system is a versatile platform designed to safeguard critical infrastructure—power and water utilities, information systems, and data centers—whether stationary or mobile. Its adaptability allows it to protect targets in transit, offering the capability to quickly reposition and deploy its "shoot and scoot" functionality. Equipped with a suite of advanced detection and engagement tools, including a remote weapon station, multi-mission hemispheric radar, electro-optical sensors, and a 70mm laser-guided rocket launcher, the EAGLS system excels in rapidly identifying and neutralizing UAS threats from a safe distance. This rapid detection-to-engagement process ensures that operators can effectively defend against aerial threats.[21]

VAMPIRE (Vehicle-Agnostic Modular Palletized Intelligence, Surveillance, and Reconnaissance Rocket Equipment). L3Harris Technologies VAMPIRE is a defense weapon that has proven effective in countering UASs and enhancing airspace security in Ukraine. This system consists of a compact rocket-launching platform equipped with a WESCAM MX-10 RSTA sensor ball and a four-shot advance precision kill weapon system (APKWS) launcher, designed to be mounted on various vehicles with flatbeds. The VAMPIRE system's key feature is its ability to launch laser-guided rockets, such as the APKWS, enabling precise engagement of enemy drones and ground threats. Notably, the system's modular and palletized design allows easy integration onto different vehicle types, offering a rapid and cost-effective solution to deploy weapons efficiently.[22]

Dedrone Tactical. Dedrone Tactical is a comprehensive anti-drone solution to address the increasing UAS threat. This agile system offers a plug-and-play approach, combining ruggedized components for RF-based detection and defeat with extended radar and camera capabilities for visual threat confirmation. The system is modular, scalable, and easy to transport, allowing quick setup and tear-down in various environments. Dedrone Tactical leverages AI-driven, autonomous C2 technology through the DedroneTracker.AI platform, providing end-to-end C-UAS kill chain capabilities. By integrating multiple sensors, including RF, radar, and cameras, Dedrone Tactical enables operators to detect, identify, track, and mitigate drone threats efficiently. The system's AI-driven, risk-based prioritization and autonomous threat confirmation features enhance airspace security by minimizing false positives and ensuring rapid responses to potential threats.[23]

Smart Shooter. Smart Shooter's C-UAS systems, particularly the SMASH 2000L and SMASH 2000+, represent advancements in countering sUAS with direct fire weapons. The SMASH 2000L is a weapon-mounted fire control system that has been integrated into the U.S. Army's C-UAS defense strategy. This system, equipped with AI, computer vision, and advanced algorithms, offers precise target elimination capabilities against ground and aerial threats. The SMASH 2000 PLUS variant includes a C-UAS mode specifically designed for the lethal elimination of small, low-flying drones.[24]

Decoys: Blending Tradition and Technology

This section delves into pragmatic, low-technology solutions aimed at enhancing the survivability of infantry and vehicular assets against such threats, alongside introducing innovative methods to deceive and disrupt enemy sUAS operations.

The 23rd Headquarters Special Troop 3133 Signal Services Company made up the "Ghost Army" of WWII, which used inflatable tanks and signal deception. This operational deception effort diverted enemy resources, ultimately preserving allied combat power. Today, Ukrainian forces have used dummies and inflatables paired with false signal emitters and other fake equipment to effectively attract and deplete Russian weapon stocks.[25]

Integrating tactical deception into offensive and defensive operations is crucial to battlefield survival. Decoys not only act as physical diversions but, when combined with EW emitters, they convincingly mimic the electronic signatures of genuine military assets. This dual-layer deception complicates the enemy's target acquisition process, forcing them to use intelligence, surveillance, and reconnaissance (ISR) resources for target verification and waste munitions on non-targets.[26] Today, advancements have led to the production of realistic, to-scale inflatable and wooden decoys by companies such as InflaTech and Metinvest, that provide realistic decoys that have optical, infrared, and radar emitting solutions.[27]

Brigade Material and Organization Decoy Recommendation

For effective LSCO, brigades should consider a comprehensive mix of inflatable and hardened decoy assets and organize a specialized team dedicated to the brigade's deception operations. This deliberate deception effort can include the following materiel and organization:

- **Essential Materiel Deception Decoys:**
    - At least one M777A2 Howitzer Battery
    - One Q-53 Radar and one Q-64 Radar
    - One command post decoy paired with electromagnetic spectrum (EMS) emitters
- **Brigade Organization Deception Section:**
    - A dedicated section, structured into two squads, specializing in the setup and movement of decoys for deception operations
    - Attached to the headquarters and headquarters company (HHC) of the brigade
    - Deployed under the directive of the brigade operations officer to integrate and quickly implement deception strategies aligned with friendly maneuvers

Benefits of decoy operations include:

- Complicates the enemy's targeting process by introducing uncertainty and complexity into the adversary's decision making
- Consumes enemy ISR resources by diverting enemy ISR efforts toward verifying targets
- Induces munition waste on false targets by misdirecting enemy firepower away from true high-value assets, increasing the survivability of those assets[28]

The cost of decoy operations is that decoy devises must be moved on the battlefield and require truck space, which is often limited in infantry brigade combat team (IBCT) and light brigade combat team (LBCT) formations. Additionally, decoys require the Soldier power for setup and tear down.

End Notes

1. Air Force Materiel Command, *Air Force Small-Unmanned Aircraft Systems Guide & Reporting Procedures*, retrieved 20 May 2024, https://media.defense.gov/2022/Mar/14/2002956012/-1/-1/1/SUAS%20IDENTIFICATION%20AND%20REPORTING%20GUIDE.PDF/SUAS%20IDENTIFICATION%20AND%20REPORTING%20GUIDE.PDF.

2. Maj. Gen. Vowell, Joel B., Maj. Anthony Padalino, Army University Press, Military Review, *Advancing the U.S. Army's Counter-UAS Mission Command Systems to Keep Pace with Modern Warfare*, May-June 2024, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2024/MJ-24-Modern-Warfare/.

3. Thales Raytheon Systems, *AN/MPQ-64 Sentinel Overview*, https://www.radartutorial.eu/19.kartei/04.battle/pubs/mpq_64.pdf.

4. Raytheon's AN/MPQ-64 Sentinel radars, retrieved 20 May 2024, https://www.rtx.com/raytheon/what-we-do/land/sentinel-radar.

5. Lockheed Martin's Q-53 Multi-Mission Radars, retrieved 20 May 2024, https://www.lockheedmartin.com/en-us/products/tpq-53.html.

6. Raytheon's Ku-Band Radio Frequency System (KuRFS), retrieved 20 May 2024, https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/kurfs.

7. Maj. Padalino, Anthony, U.S. Army.

8. Ibid.

9. Ibid.

10. Army Techniques Publication (ATP) 3-01.81, *Counter-Unmanned Aircraft Systems (C-UAS)*, 11 August 2023.

11. Joint Publication (JP) 3-10, *Joint Security Operations in Theater*, 25 July 2019.

12. JP 3-52, *Joint Airspace Control*, 22 October 2022.

13. Maj. Padalino, Anthony, U.S. Army.

14. Ibid.

15. Ibid.

16. Serohina, Kateryna, RBC Ukraine, S*hahed attack: All Russian drones shot down on approaches to Kyiv*, 21 July 2024, https://www.msn.com/en-us/news/world/shahed-attack-all-russian-drones-shot-down-on-approaches-to-kyiv/ar-BB1qlNYC?ocid=BingNewsSerp.

17. ATP 3-01.81, *Counter-Unmanned Aircraft Systems (C-UAS)*, 11 August 2023.

18. Flex Force Enterprises LLC, https://flexforce.us/dronebuster/.

19. Raytheon, *Meet the U.S. Army's LIDS: A sure shot against drones*, 8 February 2024, https://www.rtx.com/raytheon/news/2024/02/08/meet-lids-a-sure-shot-against-drones.

20. Anduril, retrieved 20 May 2024, https://www.anduril.com/roadrunner/.

21. MSI Defense Solutions, retrieved 20 May 2024, https://www.msidefense.com/eagls-c-uas/.

22. L3 Harris, retrieved 20 May 2024, https://www.l3harris.com/all-capabilities/vampire.

23. Dedrone Tactical, retrieved 20 May 2024, https://www.dedrone.com/.

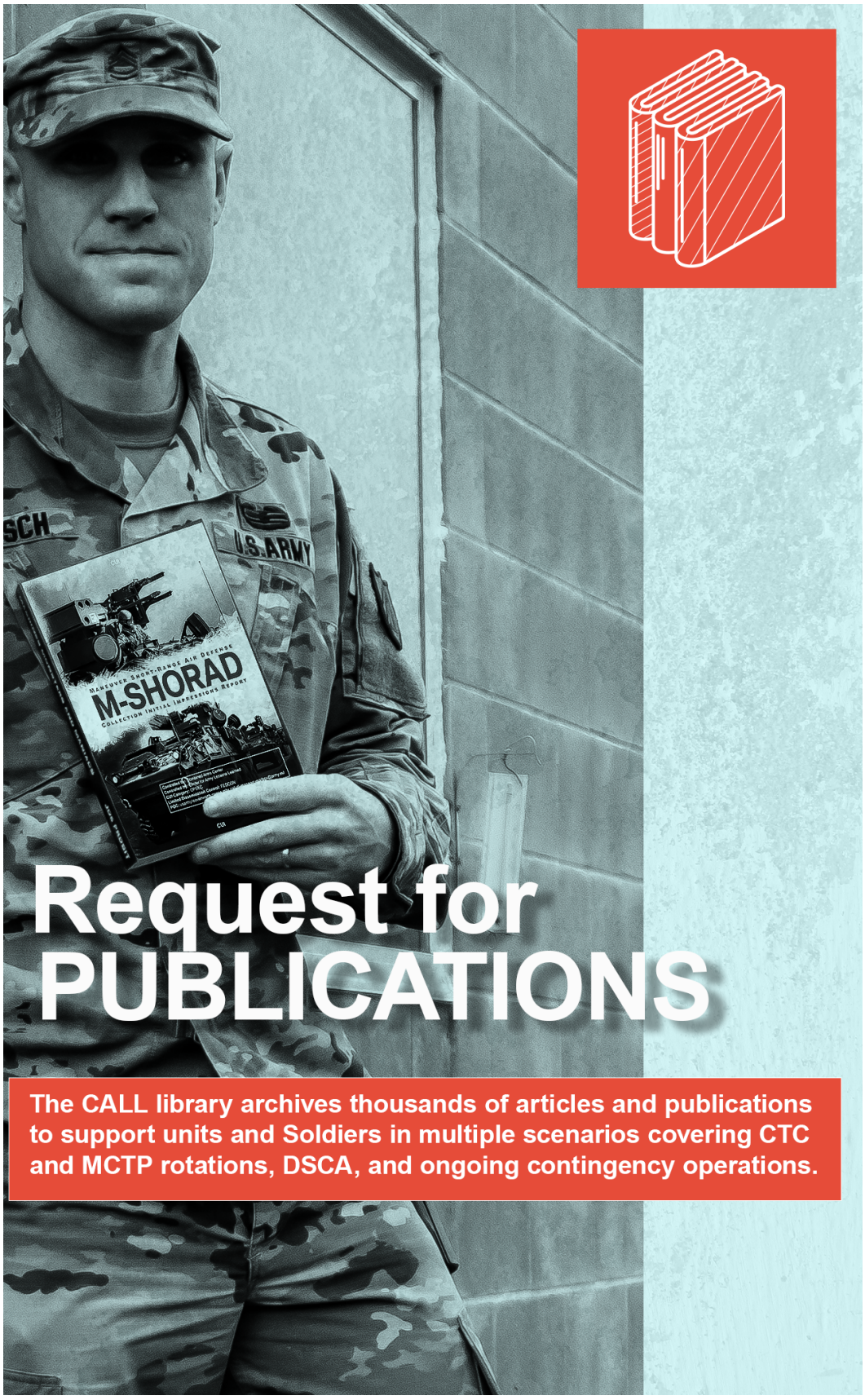
24. Smart Shooter, retrieved 20 May 2024, https://www.smart-shooter.com/.

25. Coles, Isabel, The Wall Street Journal, *How Ukraine Tricks Russia Into Wasting Ammunition*, 2 October 2023, https://www.wsj.com/world/how-ukraine-tricks-russia-into-wasting-ammunition-799ed95f.

26. Watling, Jack, Bloomsbury Publishing, *The Arms of the Future: Technology and Close Combat in the Twenty-First Century,* 5 October 2023.

27. Master Sergeant Rivero, Jorge L., U.S. Naval Institute, Vol. 150/4/1,454, *Decoy Warfare: Lessons and Implications from the War in Ukraine*, April 2024, https://www.usni.org/magazines/proceedings/2024/april/decoy-warfare-lessons-and-implication-war-ukraine.

28. Ibid.


M-SHORAD
Maneuver Short-Range Air Defense
Collection Initial Impressions Report
U.S. ARMY
Request for
PUBLICATIONS
The CALL library archives thousands of articles and publications to support units and Soldiers in multiple scenarios covering CTC and MCTP rotations, DSCA, and ongoing contingency operations.

CHAPTER 3

Brigade C-UAS Training Overview—A Recommended Concept

This section outlines a senior leader counter-unmanned aircraft system (C-UAS) education plan, and a progressive training strategy structured for a brigade to effectively implement the C-UAS process. The training plan delineates unit and institutional-level training methodologies, structured to evolve from individual Soldier training up to combat training center rotations. The training plan is detailed and directive but designed to be adaptable. Units should tailor their training programs to fit their specific mission requirements, command and control (C2) systems, and the continuously evolving sUAS threat landscape. Before a brigade deployment that has base defense as part of their mission, or a rapid fielding of emergent C-UAS technology, senior leaders of the brigade should seek education from the program management office overseeing the equipment they will operate. The section below highlights the recommendation for senior leader education on C-UAS equipment and processes. Figure 3-1 depicts a C-UAS training strategy for the brigade from individual through brigade collective training.

SENIOR LEADER EDUCATION

Senior brigade leaders scheduled to assume base defense missions in U.S. European Command (USEUCOM), or U.S. Central Command (USCENTCOM) should participate in a one-week executive course if Program Executive Office Missiles and Space or the agencies under them maintain, emplace, and service them. Program Executive Office Missiles and Space hosts this training on-site in Huntsville, Alabama, to provide commanders with direct, face-to-face interaction with leaders and hands-on insight into the operational intricacies and logistical support structures of the C-UAS equipment they will use. At a minimum, this course should do the following:

- Update commanders on the tactics and capabilities of latest C-UAS technologies
- Introduce commanders to resources like joint analysis team engineers, who offer technical expertise and feedback on employing non-program of record equipment

Additionally, commanders responsible for fixed site defense will learn to proficiently engage with the agencies listed below under Program Executive Office Missiles and Space program to understand and enhance their defensive capabilities:

- Integrated Fires Rapid Capability Office
- Integrated Fires Mission Command
- Project Manager Shield
- Project Manager Stare
- Strategic And Operational Rockets and Missiles
- Tactical Aviation and Ground Munitions Project Office

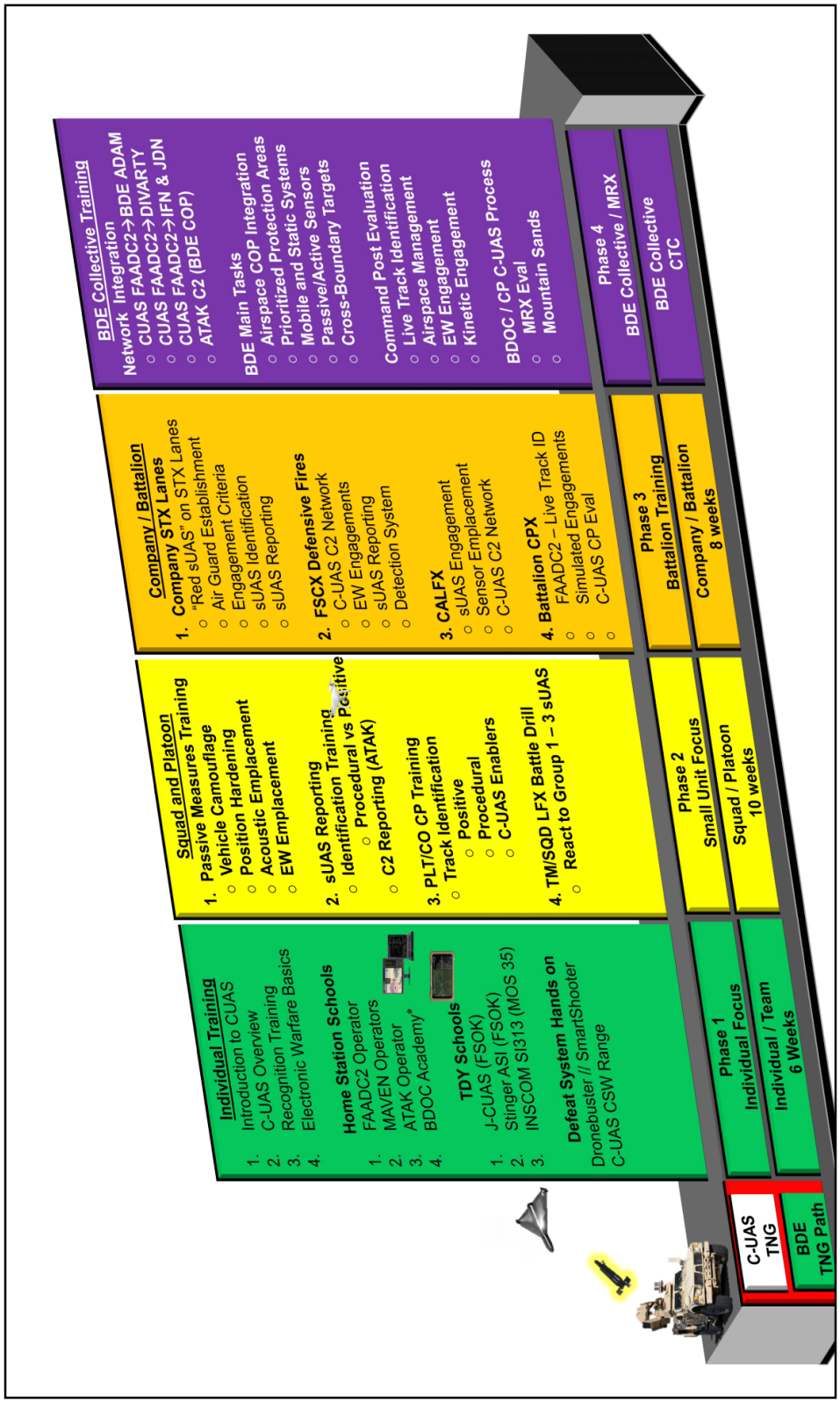


Figure 3-1. Brigade C-UAS progressive training strategy[1]

INDIVIDUAL TRAINING

Introductory training equips individual Soldiers with the essential knowledge and skills to detect, identify, and counter unmanned aircraft system (UAS) threats. This foundational training emphasizes the critical role of every Soldier in contributing to unit-wide C-UAS operations through foundational understanding and practical application.

Scope

Unit individual training should include a series of structured modules provided by instructors who have attended the joint-UAS university. The introductory training provides Soldiers with a comprehensive understanding of UAS types, capabilities, threats, and countermeasures. The curriculum should cover the following key areas:

- **Introduction to UAS and C-UAS Operations:** Overview of UAS technology, classifications, and vulnerabilities.
- **Recognition Training:** Techniques for visual and auditory identification of UAS.
- **Electronic Warfare Basics:** Fundamentals of jamming and spoofing as countermeasures.
- **Handheld C-UAS Devices:** Operational training on portable C-UAS technologies.
- **Reporting Procedures:** Standardized communication protocols and the use of C2 systems to properly report and classify detected and identified small, unmanned aircraft systems (sUASs).

Objectives

Upon completion of the individual training, Soldiers will be able to do the following:

- Understand the diverse types and capabilities of UAS and the potential threats they pose
- Identify common UAS through sight and sound with a high degree of accuracy
- Apply basic electronic warfare (EW) tactics to disrupt UAS operations
- Operate handheld C-UAS devices effectively in a field environment
- Complete reporting procedures for UAS sightings and engagements using voice and digital C2 systems (android team awareness kit [ATAK])

SQUAD AND PLATOON-LEVEL TRAINING

Squad and platoon-level training is designed to enhance capabilities in employing passive measures, effective reporting, and tactical-level command post operations against UAS threats. Building on individual Soldier training, this phase aims to certify squads and platoons to conduct the C-UAS process at their level.

Scope

Units should complete training in a series of focused modules with instructors who graduated from the joint C-UAS university at Fort Sill, Oklahoma. The structure of modules will equip squads and platoons with the skills needed to implement passive defensive measures, accurately report sUAS sightings, and manage C-UAS operations from a command post perspective. The passive measures training curriculum should include the following:

- Vehicle Camouflage: Techniques to conceal vehicles from UAS surveillance
- Position Hardening: Strategies to fortify positions against UAS threats
- Acoustic Emplacement: Use of sound to mask operational noise or mislead UAS
- EW Emplacement: Deployment of EW assets to disrupt UAS operations

C-UAS equipment qualification training will train Soldiers on procured or enabled lethal equipment, such as electronic advanced ground launcher system (EAGLS), low, slow, small, unmanned aircraft integrated defeat system (LIDS), and EW equipment, such as Dedrone Tactical. This training will include:

- LIDS tables will follow U.S. Army LIDS gunnery doctrine. Gated training for countering UAS threats using lethal, non-lethal, physical, and non-physical methods is provided in a C-UAS training circular (TC).
- Industry-provided/procured equipment hands-on training.
- C2 system training (ATAK and MPU5).

sUAS reporting training includes:

- **Identification Training:** Enhancing skills in visually and audibly identifying UAS.
- **Procedural Versus Positive:** Understanding the difference and importance of procedural and positive identification.
- **C2 Reporting (ATAK):** Standardized communication protocols using ATAK for efficient reporting and classification of sUAS.

Platoon and company command post training includes:

- **Track Identification:** Techniques for tracking and identifying UAS threats.
- **Positive Identification:** Confirming UAS threats through visual or other confirmatory means.
- **Procedural Identification:** Using operational procedures to identify potential UAS threats.
- **C-UAS Enablers:** Understanding and using available C-UAS technologies and assets within command post operations.

Team/squad live fire exercise battle drill training includes:

- **React to Group 1 – 3 sUAS:** Practical drills on responding to sUAS threats of varying classifications, focusing on rapid detection, identification, and engagement procedures.

Objectives

By the end of the training, squads and platoons will be able to do the following:

- Implement passive measures to reduce visibility to UAS surveillance and attack
- Operate provided C-UAS sensors and defeat equipment
- Report sUAS sightings using procedural and positive identification methods
- Operate effectively within a command post environment to track, identify, and make command decisions on sUAS threats
- Conduct live fire exercises that simulate real-world sUAS threat scenarios, testing the unit's response and coordination

Implementation

Duration: The training window spans 10 weeks, with each module designed for in-depth coverage and practical application.

Location: Conducted at designated training areas equipped for classroom instruction and field exercises.

Instructors: A combination of experienced Soldiers and subject matter experts from the joint C-UAS university.

COMPANY AND BATTALION-LEVEL TRAINING

This training integrates skills developed from individual to platoon level and tests the C-UAS process across the company. The battalion should use company situational training exercises as an opportunity to train their command posts in the C-UAS process, including the employment of physical and non-physical defeat systems assigned to the battalion. Testing of passive methods, the C-UAS C2 network, and the C-UAS process within the battalion will enable success at the brigade culminating training event (CTE).

Collective Training Events

Company Situational Training Exercise Lanes include:

- "Red sUAS" on STX Lanes: Integration of sUAS threat simulation into field exercises for tactical engagement practice
- Air Guard Establishment: Training designated personnel to act as air guards for sUAS detection and early warning
- Engagement Criteria: Defining clear rules for sUAS engagement in line with mission objectives
- sUAS Identification: Skill development in identifying sUAS characteristics by sight and sound
- sUAS Reporting: Instruction on effective communication methods for sUAS encounters using standardized protocols and C2 systems

Battalion Command Post Exercises include:

- **FAAD C2—Live Track Identification:** Real-time tracking and identification of sUAS with the FAAD C2 system during exercises.
- **Simulated Engagements:** Engaging sUAS in simulated scenarios to test responsiveness and decision making
- **C-UAS Command Post Evaluation:** Assessing command post processes in directing and managing C-UAS tasks

Objectives

Soldiers and units will achieve the following capabilities:

- Operate within C-UAS procedures, contributing to a collective defense against UAS threats
- Identify and report sUAS accurately and rapidly to mitigate potential threats
- Apply integrated EW techniques for sUAS neutralization
- Employ and manage C-UAS technologies within a C2 framework

BATTALION COMMAND POST AND BRIGADE-LEVEL TRAINING

Battalion command post and brigade-level training will test the brigade and battalion C2 node's ability to plan, coordinate, and execute comprehensive C-UAS operations in a complex battlefield environment.

Key components of this training include:

- **Command Post Exercises:** Simulations focused on C2 of C-UAS operations at the brigade level.
- **Mission Readiness Exercise:** Simulated C-UAS events conducted by BDOCs and/or battalion and brigade command posts.
- **Multidomain Operations:** Integration of C-UAS operations into larger brigade-level maneuvers and mission planning (combat training center rotation).
- **Inter-Brigade Coordination:** Training in cooperation with other brigades for area-wide C-UAS defense.
- **Real-World Scenarios:** Using "Red Teams" to attack brigade formations during CTEs and combat training center rotations.

Fire support coordination exercise defensive fires include the following:

- **C-UAS C2 Network:** Operational training in the use and management of C-UAS C2 networks.
- **Electronic Warfare Engagements:** Hands-on training in employing EW assets for sUAS disruption.
- **sUAS Reporting:** Drilling accurate and swift reporting procedures within the context of defensive operations.
- **Detection System:** Familiarization with the employment and operation of sUAS detection equipment.

Combined arms live fire exercises include:

- **sUAS Engagement:** Live exercises simulating sUAS threats to refine engagement strategies.
- **Sensor Emplacement:** Training on the strategic placement and use of sensors for sUAS detection.
- **C-UAS C2 Network:** Real-world application of C-UAS C2 systems in a live-fire environment.

The following are necessary for continuous learning and adaptation:

- **Feedback Mechanisms:** Regularly scheduled feedback sessions and updates to training curriculum based on emerging threats and technological advancements.
- **Cross-Training:** Exchange programs with units experienced in C-UAS operations to share best practices and lessons learned.

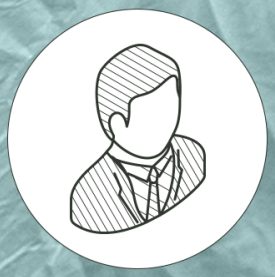
Support and resources include:

- **Simulation Technology:** Investment in mission training centers' ability to construct mock command posts or BDOCs using unit C2 systems paired with simulation technologies to create realistic UAS threat scenarios.
- **Expert Instructors:** Engagement with C-UAS experts for specialized training sessions.

End Note

1. Maj. Padalino, Anthony, U.S. Army.

OUR SERVICES



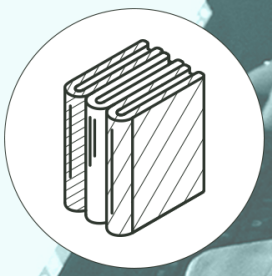
BE AN AGENT FOR CHANGE

WORKING FOR CALL

Work with us to drive Army change and impact Soldiers. Join us as a CALL Military Analyst (Forward) at a COMPO 1 active division or corps headquarters! Highly motivated self-starters currently serving in the rank of KD-qualified major or colonel (O4-O6) or master sergeant to sergeant major (E8-E9) are encouraged to apply. Soldiers selected will serve as a critical link between operational and institutional forces.

REQUEST FOR INFORMATION

CALL provides a unique service to the force by providing research and answers on a wide variety of topics. Reach out to us with your questions and your topics of interest.operations.



REQUEST FOR PUBLICATION

The CALL library is home to thousands of articles and publications. Our materials support units and Soldiers in multiple scenarios covering CTC and MCTP rotation, DSCA, and ongoing contingency operations.

CHAPTER 4

Final Thoughts

The evolving tactics of unmanned aircraft systems (UASs) on the modern battlefield necessitates advanced counter-unmanned aircraft system (C-UAS) tactics, techniques, and procedures (TTP) at the brigade level and below. The 2nd Infantry Brigade Combat Team (IBCT), 10th Mountain Division (2/10 MTN), through its recent deployment, has provided invaluable insights into the operational challenges with technical and tactical solutions in defending against UAS threats at fixed sites. This paper consolidated their experiences and applied the fixed site lessons to enhance the U.S. Army's C-UAS capabilities at the brigade and below for large-scale combat operations (LSCO).

KEY FINDINGS AND RECOMMENDATIONS

1. Integration of doctrinal solutions into brigade C-UAS operations:

Application of effective C-UAS processes is done at every echelon, from fire team to brigade command post.

Army Techniques Publication (ATP) 3-01.81, Counter-Unmanned Aircraft Systems (C-UAS), emphasizes passive measures such as position hardening, use of decoys, and operating in a dispersed manner to protect forces from hostile unmanned aircraft. ATP 3-01.81 details the active defensive C-UAS framework of detect, identify, decide, defeat, which is essential for efficient C-UAS operations at echelon.[1] Detection relies on a mix of active and passive sensors, with a focus on early warning and real-time intelligence collection. Effective planning of detection assets is critical, as it provides the necessary lead time for subsequent identification and engagement phases. Identification must balance procedural and positive methods, ensuring timely and accurate classification of UAS threats. Procedural identification, augmented by leveraging brigade-level radars and command and control (C2) systems, such as the forward area air defense (FAAD), enables operators to analyze tracks using the bearing, altitude, range, and speed (BARS) methodology. Combining techniques ensures friendly, neutral, and hostile UAS are correctly categorized, minimizing risk of fratricide, and optimizing resource allocation.

Field Manual (FM) 3-01, Air and Missile Defense Operations, details the principles and tenants of sensor employment and defeat mechanisms brigades apply within their areas of operations (AOs). The principles guide the deployment and employment of C-UAS assets, ensuring a balanced and comprehensive C-UAS defense strategy exists throughout the formation.[2]

2. Establishing brigade networks:

Establishing robust networks that can pass real-time passive and active radar data through the android team awareness kit (ATAK) into C2 systems like FAAD C2, Lattice-OS,[3] and MAVEN is vital. These networks should operate via secure but unclassified channels that can pass one-way data to secure battalion and brigade networks to ensure the seamless cueing of fire control radars and provide instantaneous detection capabilities across all echelons. By using MPU5s to establish mobile ad hoc networks (MANETs) with data pathways through mobile broadband kits, Starlink/ Starshield, Kymetta, and tactical radios, brigades will create resilient communication networks. These networks allow the integration of passive sensor data into the broader C2 infrastructure, facilitating early warning and enabling active C-UAS measures. The establishment of a robust network ensures adjacent units and higher command echelons receive critical sensor track data that enhances overall situational awareness for C-UAS operations.

3. Training and education:

A robust training strategy is paramount for developing C-UAS proficiency at all levels. Individual Soldiers must be equipped with foundational knowledge and practical skills to detect, identify, and counter UAS threats. This training should progress from basic recognition techniques to advanced electronic warfare (EW) tactics and the operation of lethal and non-lethal C-UAS equipment. Progressive training should include individual skills, squad- and platoon-level operations, and comprehensive brigade-level exercises with surrogate drones as live targets. Training modules should be structured to build in complexity, culminating in complex scenarios that simulate real-world conditions in which C-UAS and offensive fires are happening simultaneously.

Senior leaders must undergo dedicated education programs to familiarize themselves with the latest C-UAS technologies and operational procedures. A one-week executive course hosted by Program Executive Office Missiles and Space in Huntsville, Alabama, is recommended for commanders assuming base defense missions. This course provides direct interaction with experts and hands-on experience with C-UAS equipment, ensuring leaders are well-prepared to oversee and enhance their units' defensive capabilities.

CONCLUSION

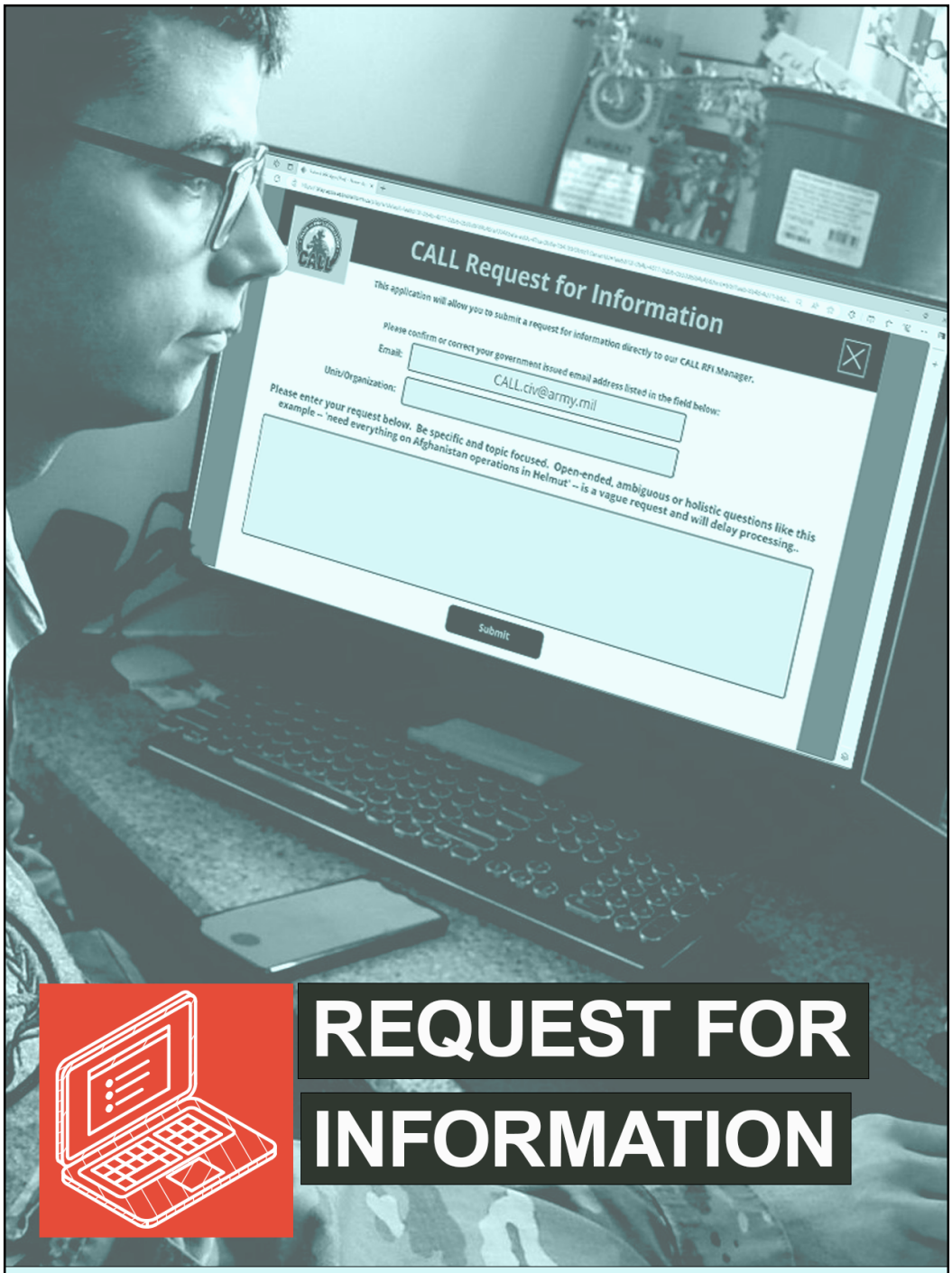
This paper outlines a clear path forward for U.S. Army brigades to enhance their C-UAS capabilities. By integrating doctrinal principles with advanced C2 systems and a structured training regimen, brigades can effectively counter the diverse and evolving UAS threats on the modern battlefield. The lessons learned by the 2nd IBCT, 2/10 MTN, offer a valuable blueprint for future operations, emphasizing the importance of adaptability, integration, and continuous learning in C-UAS operations. Implementing these recommendations will ensure that U.S. Army brigades are able to defend against adversary UAS to preserve the combat power required to fight and win in LSCO. Although the UAS threat will continue to evolve, the TTP and recommendations discussed lay a foundation for advancements in C-UAS operations at the brigade level and below.

End Notes

1. Army Techniques Publication (ATP) 3-01.81, Counter-Unmanned Aircraft System (C-UAS), 11 August 2023.

2. Field Manual (FM) 3-01, Air and Missile Defense Operations, 22 December 2020.

3. Anduril, retrieved 11 June 2024, https://www.anduril.com/command-and-control/.


CALL Request for Information
This application will allow you to submit a request for information directly to our CALL RFI Manager.
Please confirm or correct your government issued email address listed in the field below:
Email:
CALL.civ@army.mil
Unit/Organization:
Please enter your request below. Be specific and topic focused. Open-ended, ambiguous or holistic questions like this example -- 'need everything on Afghanistan operations in Helmut' -- is a vague request and will delay processing..
Submit
REQUEST FOR
INFORMATION
The Center for Army Lessons Learned (CALL) provides a unique service to the force by providing research and answers on a wide variety of topics.

GLOSSARY

ACRONYMS AND ABBREVIATIONS

2/10 MTN	10th Mountain Division
ADAM	air defense airspace management
AGL	above ground level
AMD	air and missile defense
AO	area of operations
APKWS	advance precision kill weapon system
ATAK	android team awareness kit
ATP	Army techniques publication
BARS	bearing, altitude, range, and speed
BCT	brigade combat team
BDOC	base defense operations center
C2	command and control
CALL	Center for Army Lessons Learned
CAP	combat air patrols
COP	common operational picture
COTS	commercial off-the-shelf
CTE	culminating training event
C-UAS	counter-unmanned aircraft system
DCA	defensive counterair
DIVARTY	U.S. Army Division Artillery
EAGLS	electronic advanced ground launcher system
EMS	electromagnetic spectrum
FAAD	forward area air defense
FCR	fire control radar
FLOT	forward line of own troops
HHC	headquarters and headquarters company
IBCT	infantry brigade combat team
IFN	inter-FAAD C2 network
ISR	intelligence, surveillance, and reconnaissance
JDN	joint data network
JP	joint publication
KuRFS	Ku-Band Radio Frequency System
LBCT	light brigade combat team
LIDS	low, slow, small, unmanned aircraft integrated defeat system
LSCO	large-scale combat operations
MANET	mobile ad hoc network

NCOIC	noncommissioned officer in charge
OIC	officer in charge
OWUA	one-way unmanned aerial attack vehicles
PACE	primary, alternate, contingency, and emergency
RF	radio frequency
SHORAD	short-range air defense
sUAS	small, unmanned aircraft system
TTP	tactics, techniques, and procedures
UAS	unmanned aircraft system
USCENTCOM	U.S. Central Command

CUI

CENTER FOR ARMY LESSONS LEARNED

10 Meade Avenue, Building 50
Fort Leavenworth, KS 66027-1350

U.S. ARMY
COMBINED
ARMS CENTER

COMBINED ARMS
CENTER - TRAINING

NO. 24-901
August 2024

CUI