
**Counter-Unmanned Aircraft System (C-UAS)
Operations**

MAY 2025

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 3-01.81, dated 11 August 2023.

HEADQUARTERS, DEPARTMENT OF THE ARMY

This publication is available at the Army Publishing Directorate site (<https://armypubs.army.mil>) and the Central Army Registry Site (<https://atiam.train.army.mil/catalog/dashboard>).

Counter-Unmanned Aircraft System (C-UAS) Operations

Contents

	Page
Preface.....	v
Introduction.....	vii
CHAPTER 1	1
OPERATIONAL ENVIRONMENT	1
Operational Environment.....	1
CHAPTER 2	7
ROLES & RESPONSIBILITIES	7
Roles and Responsibilities	7
CHAPTER 3	15
THREAT	15
Threat Techniques.....	15
CHAPTER 4	21
PLANNING	21
Planning Considerations.....	21
Layered Defense	28
CHAPTER 5	41
PASSIVE AND ACTIVE DEFENSE	41
Passive Defense.....	41
Active Defense Planning	50
CHAPTER 6	55
AIR DEFENSE WARNINGS AND CONTROLS	55
Air Defense Warning Conditions	55
CHAPTER 7	59
SUSTAINMENT TRAINING	59
Overview.....	59

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ATP 3-01.81, dated 11 August 2023.

APPENDIX A	67
C-UAS EQUIPMENT	67
Glossary	85
References	89
Index	91

Figures

Figure. 1-1. Notional C-UAS operational view	1
Figure 1-2. Unmanned Aircraft System communication link.....	5
Figure 2-1. Example of Counter-Unmanned Aircraft System running estimate.....	11
Figure 3-1. Unmanned aircraft system intelligence surveillance reconnaissance role	16
Figure 3-2. Unmanned aircraft system direct attack	17
Figure 3-3. Unmanned aircraft system indirect attack	18
Figure 3-4. Swarm attack	19
Figure 4-1. C-UAS planning considerations.....	22
Figure 4-2. Layered defense unmanned aircraft system example.....	30
Figure 4-3. Fixed site	34
Figure 4-4. Detection and engagement ranges	34
Figure 4-5. Observation points.....	35
Figure 4-6. Unmanned aircraft system reporting flow chart.....	36
Figure 4-7. Counter-Unmanned Aircraft System time/distance engagement sequence planning considerations	38
Figure 5-1. Examples of survivability techniques.....	43
Figure 5-2. Positioning in-depth	44
Figure 5-3. Positioning linear	45
Figure 5-4. Method of estimating 20 degrees	49
Figure 5-5. Vertical scan technique	49
Figure 5-6. Horizontal scan technique	50
Figure 7-1. Counter-unmanned aircraft system training update methodology	64
Figure A-1. FS-LIDS.....	68
Figure A-2. FS-LIDS kinetic defeat solution.....	69
Figure A-3. Ku-Band Radio Frequency System (KuRFS).....	70
Figure A-4. Coyote Block 2C.....	71
Figure A-5. Counter-Remote Control Model Aircraft Integrated Air Defense Network (CORIAN).....	72
Figure A-6. Negation of Improvised Non-State Aerial-Threats (NINJA)	73
Figure A-7. Anvil.....	74
Figure A-8. Windtalker	75
Figure A-10. Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System (M-LIDS)	76
Figure A-11. High energy laser (HEL).....	77
Figure A-12. Stinger FIM-92 man-portable air defense system.....	78
Figure A-13. Bal Chatri.....	79
Figure A-14. Dronebuster.....	80
Figure A-15. Smart shooter	80
Figure A-16. Modi.....	81
Figure A-17. FAAD C2	82
Figure A-18. Rajant.....	83

Tables

Table 1-1. Unmanned aircraft system groups	3
Table 1-2. Capabilities and limitations by unmanned aircraft type.....	4
Table 2-1. Counter-Unmanned Aircraft System Warfighting Functions	8
Table 4-1. Standardized Counter- Unmanned Aircraft System Detection Report Example (SALUTE Format)	25
Table 4-2. Framework components.....	26
Table 4-3. Survivability techniques.....	33
Table 5-1. Example Counter-Unmanned Aircraft System Detection Report (SALUTE Format)	46
Table 5-2. 16-Line Report (Incident).....	47
Table 5-3. Example Unmanned Aircraft System Engagement Report.....	48
Table 5-4. Aiming Points	54
Table 7-1. Counter-Unmanned Aircraft System Training Resources.....	62

This page intentionally left blank.

Preface

Army Techniques Publication (ATP) 3-01.81 Counter-Unmanned Aircraft System (C-UAS) Operations provides operational considerations for defending against unmanned air threats for multi-domain operations. This ATP offers planning and integration guidance for counter-unmanned aircraft system (C-UAS) platforms in a layered defense, along with both active and passive defense techniques for countering the unmanned aircraft system (UAS) threat in various areas of operations. This ATP also provides guidance on how to plan for, and incorporate, C-UAS Soldier tasks into unit training events.

The principal audience for ATP 3-01.81 is brigade and below commanders and staff, junior leaders, platoons, and individual squads who employ combined arms planning techniques within their operations (refer to ATP 3-01.8). Leaders in all organizations can benefit from C-UAS techniques prescribed in this publication. Trainers and educators will also use this publication to support the development and introduction of combined arms for air defense into existing curricula. Other services and joint organizations may use this manual to gain insight into Army air and missile defense (AMD) operations for C-UAS.

Commanders, staffs, and subordinates ensure that their decisions and actions comply with applicable United States, international, and in some cases, host-nation laws and regulations. Commanders at all levels ensure that their Soldiers operate in accordance with the law of war and the rules of engagement. (Refer to FM 6-27/MCTP 11-10C.)

ATP 3-01.81 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. ATP 3-01.81 does not prescribe any proponent terms within this publication. For other definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition. All air defense artillery-unique acronyms, with the exceptions of ADA and AMD, are spelled out the first time they are used in each of the chapters to enhance readability. Common acronyms are spelled out only once, the first time they are used.

ATP 3-01.81 applies to the Active Army, Army National Guard, and United States Army Reserve unless otherwise stated.

The proponent of ATP 3-01.81 is the Commanding General, United States Army Fires Center of Excellence and Fort Sill (USAFCoEFS). The preparing agency is the Directorate of Training and Doctrine, Air Defense Artillery Branch. Send written comments and recommendations on a DA form 2028 (Recommended Changes to Publication and Blank Forms) to Directorate of Training and Doctrine, 700 McNair Avenue, Suite 128 ATTN: ATSF-DD, Fort Sill, OK 73503; by email to usarmy.sill.fcoe.mbx.dotd-doctrine-inbox@army.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Introduction

ATP 3-01.81 establishes how the Army prevents threat UAS from impacting Army operations. Threat UAS are a condition of the modern battlefield that must be accounted for by leaders and Soldiers at every echelon. Countering unmanned aircraft systems is not a stand-alone effort or the sole responsibility of any warfighting function or branch. C-UAS is part of local security and counter-reconnaissance missions that is the responsibility of every Soldier and unit. C-UAS is not just when unmanned aircraft vehicles are flying, but also takes place “left of launch” and is part of the predictive analysis that intelligence sections do as part of their threat analysis and is incorporated into the targeting process.

Every echelon contributes to Soldier survivability by creating a layered defense. This layered defense is a combination of active and passive measures that prevents threat UAS from detecting, targeting, or destroying its intended target. Every action taken at each echelon makes the threat UAS harder to employ by increasing its risk and range it travels to accomplish its mission.

Enemy UAS is not a unique threat. The actions Soldiers take to counter-unmanned aircraft systems are not very different than actions taken to counter any other air threat such as an enemy fixed-wing or rotary-wing aircraft. While there are many systems at division and above dedicated to counter enemy air threats, each echelon works to ensure that every Soldier—no matter where they are on the battlefield, has the necessary information and ability to detect, identify, decide, and if needed to engage any air threat.

ATP 3-01.81 contains five chapters and three appendices that address: the operational environment and threat, planning and integrating C-UAS operations, passive defense techniques, active defense techniques, techniques for warning and control, attacking the network, and unit training.

- Chapter 1 discusses the Operational Environment.
- Chapter 2 discusses Roles and Responsibilities for C-UAS Operations.
- Chapter 3 discusses Threat.
- Chapter 4 discusses Planning Techniques.
- Chapter 5 discusses Passive and Active Defense.
- Chapter 6 discusses Air Defense Warnings and Controls.
- Chapter 7 discusses Sustainment Training.
- Appendix A C-UAS Equipment.

This page intentionally left blank.

Chapter 1

Operational Environment

The exponential growth of UAS creates new risks for the Army. Technology trends are dramatically transforming legitimate applications of UAS while simultaneously making them increasingly capable weapons in the hands of state actors, non-state actors, and criminals. Small UAS may also pose hazards to Army operations across all domains when controlled by negligent or reckless operators. The Army must protect and defend personnel, facilities, and assets in an environment where increasing numbers of UAS will share the skies with standard aircraft, operate in the airspace over Army installations, and be employed by our Nation's adversaries.

This chapter describes the operational environment in which ground units at all levels must plan, coordinate, and synchronize actions to UAS threats. The UAS threat continues to advance technologically and have proliferated exponentially over the past decade. As technology has progressed, both reconnaissance and attack capabilities have matured to the point where enemy UAS represent a significant threat to Army, joint, and multinational partner operations from both state and non-state actors. Figure 1-1 depicts a notional C-UAS operational view.

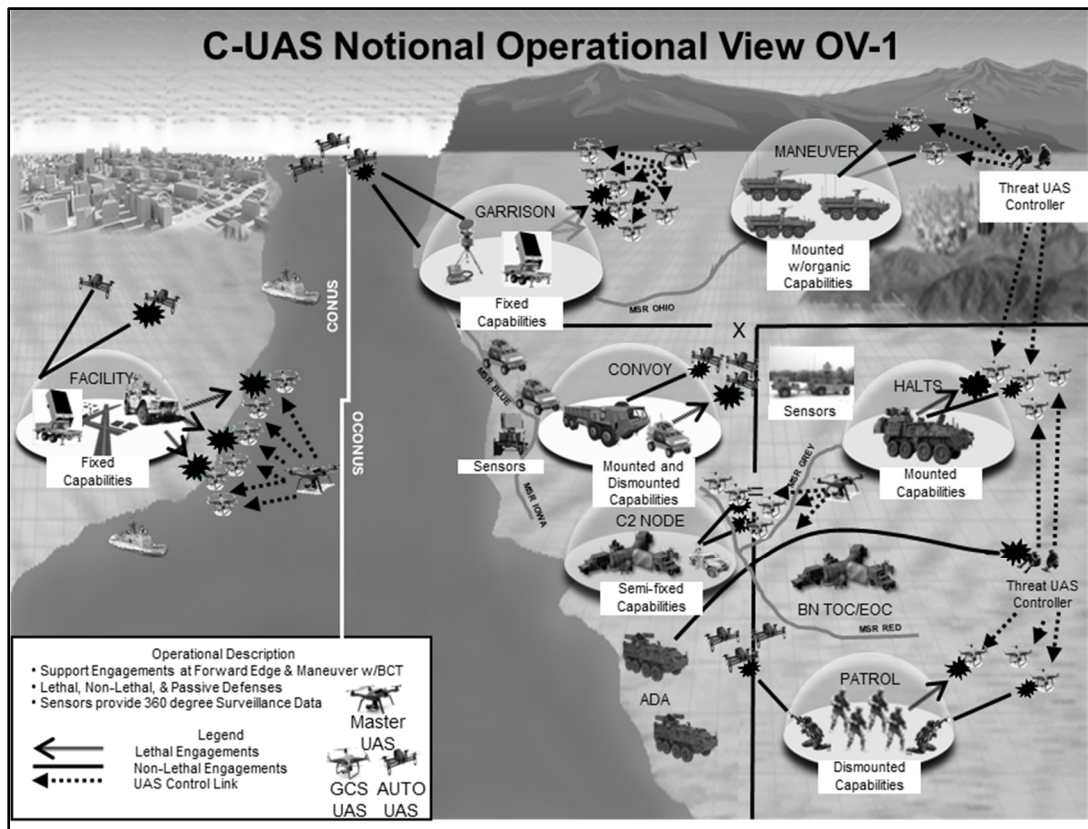


Figure 1-1. Notional C-UAS operational view

OPERATIONAL ENVIRONMENT

1-1. The *operational environment* is the aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander (JP 3-0). The operational environment (OE) includes enemy, friendly, and neutral elements. This environment must be understood

across the entire competition continuum, from peace to war, and across the entire range of military operations, from military engagement, security cooperation or deterrence mission to multi-domain operations (see FM 3-0 for further discussion on OE).

1-2. Commanders and planners must understand the physical environment, governance, technology, local resources, and culture of elements within the area of operations (AO). They must then translate this understanding into actionable mission orders to their units. Defining and understanding the OE enables the staff to focus their planning efforts on defending against low-level air threats and assists the unit in creating an effective C-UAS strategy.

1-3. Commanders and staffs require information that allows them to understand and influence the environment where their forces operate. They use this information as a basis to fill information requirements, complete thorough assessments, develop and refine plans, and conduct operations. Specific to C-UAS, commanders and staffs must apply methods that identify the effects UAS have within the OE on friendly and enemy courses of action to include:

- Determining likely avenues of approach.
- Identifying potential target areas.
- Estimating threat UAS standoff ranges.
- Employing layered C-UAS capabilities based on OE factors.

UNMANNED AIRCRAFT SYSTEM COMPONENTS

1-4. *Unmanned aircraft system* is a system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft (JP 3-30). A UAS is controlled remotely through a specific datalink. An unmanned aircraft (UA) is an aircraft that can fly autonomously or remotely. UAS is the totality of everything that makes up a UA platform including its position, navigation, and timing (PNT) module, ground control module, transmission systems, camera, all software, and the operator on the ground controlling the UAS.

1-5. As depicted in the table below, UAS are categorized into Groups 1 through Group 5, and this designation is typically based on weight, operating altitude, and speed. The bigger the platform the more robust its suite of capabilities. This ATP focuses on Groups 1 through 3. While the group designations can clarify UAS and their capabilities, it is important that commanders and staff understand that lines of differentiation between the groups operationally are not rigid. Both passive and active defense efforts should include capabilities that provide overlapping, redundant protection against all UAS threats. See table 1-1 for a brief description of the UAS groups.

Table 1-1. Unmanned aircraft system groups

Group	Weight (lbs)	Speed (kts)	Normal Operating Altitudes	Notes	Threat & COTS Examples	Friendly Examples
Group 1: micro/mini UAS	0 - 20	<100	< 1,200 AGL	Generally, hand launched, possibly commercial-off-the-shelf, radio-controlled platforms. They have limited ranges and small payload capabilities. They offer real time video. Operated within line of sight of the user.	DJI MAVIC, Enterprise Dual	RQ-11 Raven
Group 2: small tactical UAS	21 - 55	101 - 250	< 3,500 AGL	Small airframes with low radar cross sections provide medium range and endurance. Launched from unimproved areas with a small number of people involved. Typically line of sight to the ground control station.	SKY-09Ps	Scan Eagle
Group 3: Tactical UAS	56 – 1,320		< 18,000 AGL	Similar to Group 1 and 2 UAS, requires a larger logistical footprint. Range and endurance vary significantly among platforms.	Shahed 136	RQ-7B Shadow
Group 4: Strategic or theater UAS	> 1,320	Any speed	< AGL 18,000	Relatively large systems operated at medium to high altitudes. This group has extended range and endurance capabilities. Normally requires a runway for launch and recovery.	Forpost	MQ-1C Gray Eagle MQ-1A/B Predator
Group 5: Strategic UAS	> 1,320	Any speed	> AGL 18,000	Operates at medium to high altitudes having the greatest range, endurance, and airspeed. Requires large logistical footprint like that of manned aircraft and has a suite of optics for targeting and weaponry for engagements.	Wing Loong II	RQ-4 Global Hawk MQ-9 Reaper
AGL above ground level COTS Commercial off the shelf Kts Knots UAS unmanned aircraft system lbs pounds						

1-7. UAS are abundant, easy to proliferate, and difficult to detect on the battlefield. They constitute a significant threat facing ground forces, especially when integrated with other attack capabilities. The technological enhancements, accessibility, and economic feasibility of the UAS make them an attractive option for potential adversaries. Planners should assume that all UAS platforms can be outfitted with different suites of capabilities. These may include intelligence, surveillance, and reconnaissance (ISR), command and control (C2), targeting capabilities, electro-optical or infrared optics, radar, signals intelligence, or laser

designation supporting the delivery of electromagnetic warfare (EW), air-to-surface weapons, surface-to-surface weapons, or one-way lethal payloads (Loitering Munitions). Loitering munition is a reference to any UAS that can engage beyond line-of-sight ground targets with an explosive warhead or lethal payload to cause injury via a “suicide mode” attack.

1-8. There are three types of UAS: rotary-wing/vertical takeoff and landing, fixed-wing, and hybrid. Rotary-wings UAS operate like helicopters, so their greatest advantages are their vertical flight capability, which facilitates takeoffs and landings, and their hovering capability, which allows them to fly in narrow spaces and around obstacles. A fixed-wing UAS can fly at a higher altitude than other UAS. It will typically have greater ranges and is more efficient than its rotary-wing counterparts are and is thus often better suited for surveying larger plots of ground or geography on a single flight. A hybrid UAS is a combination of a fixed and rotary-wing UAS that can hover like a rotary-wing and fly like a fixed-wing. The advantages are they can conduct vertical take-off in addition to flying like a traditional fixed-wing aircraft (see table 1-2).

Table 1-2. Capabilities and limitations by unmanned aircraft type

<i>Type</i>	<i>Capabilities</i>	<i>Limitations</i>
<i>Fixed wing</i>	- Increased flight time. - Larger payload capacity. - Greater speed.	- May have increased operational and sustainment requirements. - Needs room for takeoff and landing. - Must constantly move forward, not able to hover.
<i>Rotary-wing</i>	- Vertical take-off and landing capable, which means they can make off from almost anywhere. - Ability to hover and stare capability. - Requires little training. - Low cost easy to acquire and conceal.	- Low load carrying capacity. - Limited speed.
<i>Hybrid</i>	Includes advantages of fixed wing and VTOL unmanned aircraft.	Includes disadvantages of fixed wing and VTOL unmanned aircraft.

1-9. Group 1 UAS consist mostly of hand-launched radio-controlled platforms. Due to construction, range, cost, and operation, these UAS may be operated using launch and forget tactics. These tactics allow one operator to conduct limited ISR gathering operations. Adding weapons to these platforms is possible and can provide significant effects for the adversary. Additional weight, however, will change the range of the aircraft, significantly reducing its effectiveness. These Group 1 platforms are most capable of ISR gathering tasks.

1-10. Group 2 and 3 UAS are larger than micro and mini UAS. They are relatively small airframes constructed of lightweight materials. The increased size, range, and load bearing capacity of these larger UAS enable a wide range of mission and payload capabilities. This increases threat capability well beyond ISR operations.

1-11. Loitering munition is a type of UAS designed to engage beyond line-of-sight ground targets with an explosive warhead. Loitering munitions are often portable and meant to provide ground units such as infantry with a guided precision munition. They are equipped with high-resolution electro-optical and infrared cameras that enable the operator to locate, surveil, and guide the vehicle to the target. A defining characteristic of loitering munitions is the ability to "loiter" in an area of airspace for an extended period before striking, giving the operator time to decide when and what to strike.

1-12. Group 1 thru 3 UAS have a lower radar cross-section larger than Groups 4 and 5 UAS. This low radar cross-section is harder to detect by friendly forces' early warning and detection capabilities. Launch and recovery requirements allow UAS launching capability from unimproved areas by a single person or small team, making them more difficult to find. Advances in artificial intelligence capabilities enable threat actors to employ UAS with little to no operator interaction. Artificial intelligence capability is also increasing the threat of swarm attacks, highlighted in paragraph 3-2.

1-13. Rapidly advancing technology and ready availability of UAS by state and non-state actors has resulted in a significant increase in UAS threats against U.S. forces and our allies. Threat UAS information is critical and likely differs between adversaries. Commanders at all levels face the challenge of being able to counter

the air threat and adversarial reconnaissance within their OE. Countering air threats and UAS threats are shared joint and combined arms responsibilities. Commanders and staffs must be prepared to address these across the entire competition continuum (refer to FM 3-0, chapter 1 for more information on OE).

1-14. Leaders and Soldiers must understand how UAS operate and where they are vulnerable in order to plan a defense. A UAS has three main components: the sensor, the controller, and the communication links. Each component has its own weakness. The sensor is vulnerable to Global Positioning System [US system], GLONASS [Russian system], Galileo [EU system], and BeiDou [Chinese system] signals. The controller to link protocols and the communications link are vulnerable to video and telemetry downlink. See figure 1-2, for visual representation of the communication path for a UAS.

- The sensor (UAS) relies on a commercial position, navigation, and timing PNT (L1 channel) signal for stabilization. The PNT down link is needed to establish which way is up or down and its altitude. It is required if the UAS needs to fly to a specific point if a C2 signal is not being utilized.
- The controller is not always required to operate the UAS. The C2 uplink signal can be used to geo-locate the actual operator of the UAS.
- The video and telemetry downlink signals from the UAS to the controller are one directional and these signals can be used to geo-locate the actual UAS. The signal can be intercepted using cyber effects to locate the UAS reporting location and possibly its video feed.
- Pilot in the loop operations maintains C2 via line of sight (LoS) and beyond line of sight (BLoS) methods. Autonomous operations do not need a data link, can be programmed from launch to recovery

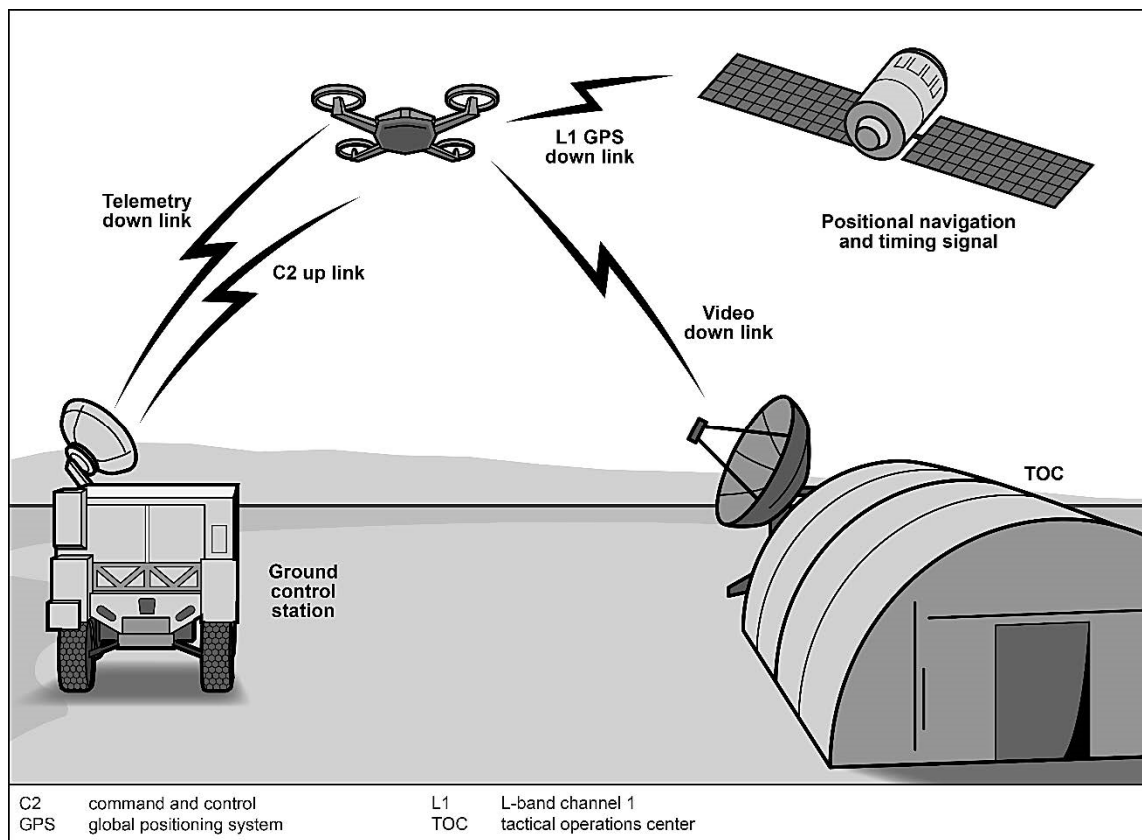


Figure 1-2. Unmanned Aircraft System communication link

1-15. Multiple devices we use operate on various waveform frequencies. When jamming, you can jam across one or more frequencies. Operators and leaders must understand what frequencies are being jammed and what other equipment may be impacted as a second or third order effect. A UAS relies on PNT signal for stabilization, lost link protocols, and video downlink/telemetry; UAS video downlink presents a weakness that may be exploited by friendly forces. Leaders must understand the electromagnetic frequency and the

factors that influence it for planning and how to mitigate the risk of potentially jamming friendly equipment.

Factors that may influence the range of signals are-

- Antenna
- Receiver noise
- Output power
- Radio pollution
- Environment
 - Line of Sight
 - Obstructions
 - Reflections
 - Atmospheric effects

Chapter 2

Roles & Responsibilities

This chapter provides guidelines for the roles and the responsibilities of commanders and specific staff to assist in developing C-UAS techniques. It discusses actions needed for preparing and to take when anticipating or encountering possible UAS threats while on the battlefield. This information complements C-UAS planning considerations, commander's intent and guidance, threat environment, and standard operating procedures.

ROLES AND RESPONSIBILITIES

2-1. Commanders direct the continuous integration of C-UAS operations whether in a tactical environment or at home station. By leveraging cyberspace operations and EW as part of the combined arms approach, commanders can sense, understand, decide, act, and assess faster than the adversary assesses and achieve a decisional advantage in multiple domains during operations.

2-2. Commanders should-

- Include C-UAS within the operations process.
- Continually enforce cybersecurity standards and configuration management.
- Understand, anticipate, and account for C-UAS capabilities, constraints, and limitations, including second and third order effects.
- Understand the legal and operational authorities to affect threat portions of C-UAS.
- Understand the implications of C-UAS operations on the mission and scheme of maneuver.
- Understand how the selected course of action affects the prioritization of resources.
- Leverage effects in and through cyberspace and the EMS to support the concept of operations.
- Develop and provide intent and guidance for actions for C-UAS.
- Identify critical terrain relevant to C-UAS that may affect critical tasks or missions by phase.
- Ensure active collaboration across the staff, subordinate units, higher headquarters, and unified action partners that enable a shared understanding of C-UAS.
- Approve collection priorities and risk mitigation measures.
- Ensure the synchronization of C-UAS with other lethal and nonlethal fires to support the concept of operations.

2-3. Warfighting functions are the physical means that tactical commanders use to execute operations and accomplish missions assigned by superior operational and tactical level commanders. The purpose of warfighting functions is to provide an intellectual organization for common critical capabilities available to commanders and staffs at all echelons and levels of warfare (ADP 3-0). Each warfighting function has requirements throughout the C-UAS planning, preparing, executing, and assessing process. See table 2-1 on page 8, for details of some of those requirements for each.

Table 2-1. Counter-Unmanned Aircraft System Warfighting Functions

Warfighting Functions	PLAN	PREPARE	EXECUTE	ASSESS
Movement & Maneuver	-Coordinate vulnerability assessment -Conduct Commander's risk assessment -Determine CCIR -Identify passive/active defense measures -Identify air guards	-Rehearse battle drill for UAS event	-Detect/Identify UAS platform -Conduct host nation coordination -Defeat	-Review TOCSOP/battle drill execution
Intel	-Conduct IPOE -Coordinate coverage beyond organic sensors -Provide input to CCIR/essential element of friendly information -Identify (ID) NAI/TAls	-Conduct sensor/information collection rehearsal synchronization drill	-Detect/Identify UAS platform	-Track UAS exploitation -Report exploitation findings -Identify trends and TTP
Fires	-Disseminate weapons control status -Establish level of control	-Rehearse clearance of fires	-Deconflict air space	
Protection	-Refine protection priorities -Update protection priority list -Establish general & local air defense warnings	-Rehearse deconfliction	-Initiate air defense warning -Deconflict air space	-Update TTP based off exploitation and trends
Sustainment	-Plan for sustainment of C-UAS systems (CL III, V, IX) -Maintenance (organic or FSR support)	-Check battery/cable status -PCC/PCI CL III, V, IX -Systems PMCS	-Sustain C-UAS systems	-Review -Issue Resupply -Order(s)
Command and Control	-Define UAS ROE -Determine identification authority -Determine engagement authority -Establish notification procedures	-Review reporting procedures -Validate PACE plan	-Execute reporting procedures along PACE	-Review reporting procedures -Review ROE -Review engagement authority
CCIR commander's critical information requirement PCI precombat inspections FSR field service representative ROE rules of engagement IPOE intelligence preparation of the operational needs statement, operational needs statement, TAI target area of interest NAI named area of interest TOCSOP tactical operations center standard operating procedure PACE primary, alternate, contingency, and emergency TTP tactics, techniques, and procedures PCC precombat checks UAS unmanned aircraft system				

STAFF ROLES AND RESPONSIBILITIES

2-4. The staff assists the commander in understanding, visualizing, and describing the OE, making decisions, and directing military operations. Staffs must conduct analysis and make recommendations based on their specific roles and areas of expertise. C-UAS operations require extensive coordination and cooperation across a wide range of staff elements. Staffs synthesize information coordinated and synchronized across multiple disciplines and areas of focus and provide it to commanders in the form of running estimates to help commanders build and maintain their situational understanding. Staff elements with critical areas of input in planning and executing C-UAS operations are outlined in this chapter.

S-2

2-5. The S-2 advises the commander and staff on intelligence aspects of C-UAS operations. Their role is to provide, timely, relevant, accurate and predictive intelligence support to enable commanders to make timely and relevant decisions. The S-2 must coordinate closely and constantly with the Division G-2 for updated threat information regarding C-UAS operations.

S-3

2-6. The S-3 is responsible for the overall planning, coordination, and supervision of C-UAS activities. Additionally, the S-3 is responsible for all matters concerning plans, operations, and training at brigade and below. The S-3-

- Plans for and incorporates C-UAS into operation plans and orders, within the fire support plan and the information operations plan (in joint operations).
- Tasks C-UAS activities to assigned and attached units.
- Exercises control over C-UAS, including electromagnetic deception plans.
- Directs EP measures based on recommendations from the S-6 staff, the cyber electromagnetic warfare officer, and the CEMA working group.
- Coordinates EW and C-UAS training requirements.
- Issues C-UAS support tasks within the information collection plan. These tasks are developed, according to the collection plan and the requirements tools, by the S-2 and the requirements manager.
- Ensures through the CEMA working group, that EW and C-UAS activities support the plan.
- Integrates EA within the targeting process.
- Integrates C-UAS into the overall protection plan via the protection cell.

S-6

2-7. The network defense technician, network management technician, information services technician, spectrum manager, and information security manager participate in planning EW techniques for C-UAS operations. The S-6-

- Assists the cyber electromagnetic warfare officer with the preparation of the EP policy.
- Reports enemy electromagnetic attack activity detected by friendly communications and electronic elements to the CEMA working group for counteraction.
- Assists the unit cyber electromagnetic warfare officer with resolving EW systems maintenance.
- Identifies and deconflicts electromagnetic interference.
- Issues the signal operating instructions.
- Ensures network connectivity for all EW computer systems.
- Provides EMS resources to the unit or task force (refer to ATP 6-02.70).
- Coordinates for EMS usage with higher echelon G-6 (S-6), communications system directorate of a joint staff, and applicable host-nation and international agencies as necessary.
- Prepares the restricted frequency list and issuance of emissions control guidance.
- Coordinates frequency allotment, assignment, and use.
- Supports the CEMA working group by assisting in the development of electromagnetic deception plans and activities that include EMS resources.
- Coordinates with higher echelon spectrum managers for EMS interference resolution.
- Assists the cyber electromagnetic warfare officer in issuing guidance to the unit, including subordinate elements, regarding deconfliction and resolution of interference problems and processes involving EW systems.
- Participates in the CEMA working group to deconflict friendly EMS requirements with EW C-UAS activities and information collection efforts.
- Supports all subordinate unit software updates and communications security requirements.
- Compiles and distributes the joint restricted frequency list (spectrum manager).
- Assists the EW section with computer maintenance and troubleshooting.

C-UAS Running Estimate

2-8. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (ADP 5-0). Information which may appear in an S-6 specific C-UAS running estimate would include committed and reserved assets, maintenance status of C-UAS equipment, and training proficiency of EW personnel. Resources that are useful in developing a running estimate are the maintenance report and the commanders' training assessments. Threat information is available from online databases, unit intelligence assets, and national intelligence sources.

2-9. The purpose of the running estimate is to provide a consolidated list of information about cyberspace and the EMS to assist other staff sections in planning, preparing, and executing operations. The information serves as a foundation and is dependent on information requirements with other staff such as operations, fires, intelligence, and signal as sources of information. Some of this information will be redundant with other staff section planning products. Figure 2-1 is an example of a C-UAS running estimate that an S-6 section might produce. All staff sections have responsibilities in conducting running estimates and other aspects of the military decision-making process during the planning for and conduct of C-UAS operations. Paramount considerations should include-

- Survivability of personnel and equipment.
- The time required to build or improve the unit's EP posture and position EA and electromagnetic support capabilities.
- Ability of C-UAS resources to achieve the desired effects.
- Reprogramming of C-UAS and EW assets.
- Capabilities, limitations, advantages, and disadvantages of available EW and signals intelligence assets equipped with electromagnetic support capability.
- Intelligence available for targeting.
- Current and projected maintenance C-UAS status.
- Facts.
- Assumptions.
- Friendly Forces status.
- Enemy Activity/capabilities.
- Civil Considerations.
- Readiness of equipment, personnel, and factors of mission accomplishments.
- Relative to your staff sections/functional areas.
- Conclusions and recommendations.

C-UAS Running Estimate	
1. Friendly electromagnetic warfare and C-UAS system. a. System nomenclature and disposition by echelon. i. Planning, modeling, and simulation tools. ii. Organic systems. iii. Echelons above corps and joint assets. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters data paths and bandwidth requirements). c. Modeling and simulation of each system based differing parameters and area of operations. i. Differing power ratios. ii. Antenna configuration. iii. Terrain. d. Constraints and limitations associated with each system. 2. Friendly spectrum-dependent system. a. System nomenclature and disposition by echelon. i. VHF radio. ii. Satellite communication terminals. iii. Radar sets. iv. Unmanned aircraft systems. b. System characteristics. i. Frequency range. ii. Bandwidth requirements. iii. Power. iv. Modulation.	
C-UAS	counter-unmanned aircraft system
	VHF very high frequency

Figure 2-1. Example of Counter-Unmanned Aircraft System running estimate

C-UAS Running Estimate	
c. Modeling and simulation of each system based on differing parameters and area of operations. d. Constraints and limitations associated with each system.	
3. Threat electromagnetic warfare and C-UAS systems.	
a. System nomenclature and disposition by echelon. b. System capabilities. i. Frequency range. ii. Modulation type(s). iii. Maximum power output. iv. Antenna configuration and characteristics. v. Command and control details (mesh network parameters, data paths, and bandwidth requirements). c. Threat electronic warfare tactics, techniques, and procedures. d. Modeling and simulation of each system based on differing parameters, and area of operations. e. Critical capabilities and vulnerabilities by system.	
4. Threat spectrum-dependent	
a. System nomenclature and disposition by echelon. b. System capabilities. i. Frequency range. ii. Bandwidth requirement. iii. Power. iv. Modulation. c. Tactics, techniques, and procedures. d. Frequency allocation. e. Cueing cycles (radar set). f. Modeling and simulation of each system, based on differing parameters and area of operations. g. Critical capabilities and vulnerabilities by system.	
5. Civil infrastructure consideration.	
C-UAS	counter-unmanned aircraft system
	VHF very high frequency

Figure 2-1. Example of Counter-Unmanned Aircraft System running estimate (continued)

Air Defense Airspace Management/Brigade Aviation Element Cell

2-10. The air defense coordination/management officer in the brigade combat team level ADAM/BAE cell is responsible for ensuring that all organic elements (staff, organic units, and attached units and personnel) understand and employ the necessary passive defense measures to mitigate the effectiveness of enemy UAS. Passive air defense measures are the first line of defense against UAS. Based on the unit's assigned mission and rules of engagement, the commander will have discretion as to engage any approaching confirmed hostile aerial platforms. The Air Defense Airspace Management/Brigade Aviation Element (ADAM/BAE) cell will also assist in the clearance for lethal UAS engagements.

Staff Judge Advocate or Representative

2-11. The staff judge advocate is responsible for all legal advice. The staff judge advocate or representative reviews all C-UAS operations to ensure they comply with existing Department of Defense directives and instructions, rules of engagement (ROE), and applicable domestic and international laws, including the law of war. They can also assist the command in requesting additional required authorities for employment of C-UAS systems.

Cyber Electromagnetic Activities Section

2-12. Cyber electromagnetic activities sections are assigned to the G-3 or S-3 within corps, divisions, brigade combat teams, and combat aviation brigades. Commanders are responsible for ensuring that CEMA sections integrate cyberspace operations and EW into their concept of operations. The CEMA section plans, coordinates, and integrates cyberspace operations and EW in support of the commander's intent. It is responsible for the coordination to deconflict spectrum management efficiency. The CEMA section collaborates with numerous staff sections to ensure unity of effort in meeting the commander's total operational objectives. The CEMA section is responsible for synchronizing and integrating cyberspace operations and EW with the operations process and through other integrating processes. Personnel assigned to the CEMA section are the-

- Cyber electromagnetic warfare officer.
- Cyber warfare officer.
- EW technician.
- EW sergeant major (corps) or EW noncommissioned officer in charge (division).
- EW noncommissioned officer.
- CEMA spectrum manager.

2-13. The CEMA section leads the CEMA working group. The CEMA working group is not a formal working group that requires dedicated staff members from other sections. When needed, the cyber electromagnetic warfare officer uses a CEMA working group to assist in synchronizing and integrating cyberspace operations and EW into the concept of operations. The CEMA section normally collaborates with key stakeholders during staff meetings established as part of the unit's battle rhythm and throughout the operations process. Membership in the CEMA working group will vary based on mission requirements.

2-14. If scheduled, the CEMA working group will integrate into the staff's battle rhythm. The CEMA working group is responsible for coordinating horizontally and vertically to support operations and assisting the fires support element throughout the execution of an operation. Generally, the CEMA working group is comprised of staff representatives with equities in CEMA, and typically includes-

- The G-2/S-2.
- The staff weather officer.
- The G-6/S-6.
- The information operation officer or representative.
- Spectrum manager.
- The fire support officer or a fires support element representative.
- The staff judge advocate.
- The protection officer.

Protection Cell

2-15. The protection cell advises, visualizes, and outlines protection requirements to the commander; prioritizes and synchronizes mitigating strategies, and coordinates protection. It recommends measures to deny enemy stand-off, reducing the degradation, disruption, and denial of friendly force operations. Primary members of the protection cell typically include the chief of protection and representatives from air and missile defense, personnel recovery, provost marshal, CBRN, EOD, engineer, medical, and antiterrorism/force protection sections.

2-16. The protection cell (supported by the protection working group) develops the scheme of protection after receiving guidance and considering the principles of protection in relation to mission variables and the

systems requiring protection. The scheme of protection is based on the mission variables thus, it includes protection priorities by area, unit, activity, or resource. It addresses how protection is applied and derived during all phases of an operation. For example, the security for routes, bases/base camps, and critical infrastructure is accomplished by applying protection assets in dedicated, fixed, or local security roles; or it may be derived from economy-of-force protection measures, such as area security techniques. It also identifies areas and conditions where forces may become fixed or static and unable to derive protection from their ability to maneuver. These conditions, areas, or situations are anticipated, and the associated risks are mitigated by describing and planning for the use of response forces.

2-17. The protection cell considers the following items, at a minimum, as it develops the scheme of protection:

- Protection priorities (critical capabilities, areas, and information).
- Air defense positioning guidance.
- Specific terrain and weather factors.
- Areas or events where risk is acceptable.
- Protected targets and areas.
- Vehicle and equipment safety or security constraints.
- Personnel recovery actions and control measures.
- Force protection condition status.
- Mission-oriented protective posture guidance.
- Environmental guidance.
- Explosive ordnance and hazard guidance.
- Ordnance order of battle.
- Operations security risk tolerance.
- Fratricide avoidance measures.
- Rules of engagement, standing rules for the use of force, and rules of interaction.
- Escalation of force and nonlethal weapons guidance for C-UAS equipment.
- Operational scheme of maneuver.
- Military deception.
- Obscuration.
- Electromagnetic spectrum status.
- Availability of personnel recovery capable assets, gaps in recovery coverage, preparation of individuals.

Chapter 3

Threat

UAS are an ever-present danger in the modern operating environment and with time the threat of UAS will continue to grow. This chapter will discuss the current ways UAS are being employed on the battlefield. This chapter discusses current threat UAS employment tactics on the battlefield.

THREAT TECHNIQUES

3-1. Tactical level UAS operate at various altitudes. The ability for groups 1 thru 3 UAS to operate at low altitudes decreases the likelihood of friendly forces detecting the threat in a timely manner. UAS provide cost effective, high payoff means of surveillance and reconnaissance for an adversary. Integrated AMD capabilities can effectively counter larger UAS groups, but have difficulty tracking, identifying, and defeating lower class UAS. The challenge is at the brigade and below level with planning for and defending against small UAS threats.

3-2. The advancements in unmanned technologies allow threat actors asymmetrical means to conduct attacks, collect information, or trigger other threatening events. This problem can escalate as UAS technologies become less expensive and more capable, accessible, and adaptable. Mass UAS employment by threat forces can produce overwhelming effects on maneuver forces. Understanding threat capabilities as well as current and emerging UAS employment tactics is critical in the effort to counter UAS threats. UAS may be employed to conduct a wide variety of missions to include ISR, direct, indirect, or mass attack, fire support, harassment/nuisance and EW:

- Intelligence, surveillance, and reconnaissance (ISR): mounted cameras; UAS can provide an adversary with a contemporary ISR capability in real time. Patterns of life, such as when there is a shift change and feeding hours, can be used in enemy target acquisition and use in the information operation campaign. See figure 3-1 on page 3-16 for depiction of UAS used in an ISR role.
- Command and control (C2): UAS can provide an aerial view of the OE to provide commands to forces to accomplish assigned missions.
- Direct attack: UAS can be employed as a fire-and-forget weapon in a "suicide mode" with either just the UAS, or with an explosive chemical biological and radiological payload attached to cause injury. See figure 3-2 on page 3-17 for depiction of UAS used in a direct attack role.
- Indirect attack: The UAS deploys a payload while maintaining overhead coverage and video feed. Payloads may include explosives, chemical or biological agents, radiological isotopes or other payloads to disrupt, attrit, and destroy friendly forces. See figure 3-3 on page 3-18 for a depiction of UAS used in an indirect attack role.
- Forward Observer: UAS can provide forward observer functionality that can enable adjustment of indirect fire or provide direct line of sight to the target. Forward observation concerns the employment of UAS for target acquisition and battle damage assessment.
- Harassment/nuisance: UAS can be used in manner that congests airspace or interdicts movement, which may be intentional or unintentional.
- Swarm/mass attacks: A swarm refers to a method of operations in which multiple, sometimes-autonomous systems act as a cohesive unit by actively coordinating their actions. A swarm of UAS is a cluster, fleet, or set of aerial UAS that work together to achieve a specific goal and are controlled either manually or autonomously. What differentiates a swarm from a group of individual UAS is the capability of the UAS within the swarm to communicate with one another and work to accomplish prescribed objectives, whereas a group is any number of UAS, each of which is being controlled by a single source. See figure 3-4 on page 3-19 for depiction of UAS used in a swarm/mass role on.
- Electromagnetic warfare: Near peer adversaries are increasingly investing in EW capabilities to include UAS based EW platforms. Uses include electromagnetic support (radio direction finding, threat recognition) and electromagnetic attack (EA) (jamming, spoofing). Jamming communications

can add to the battlefield confusion resulting in reduced friendly command and control while the threat conducts offensive operations.

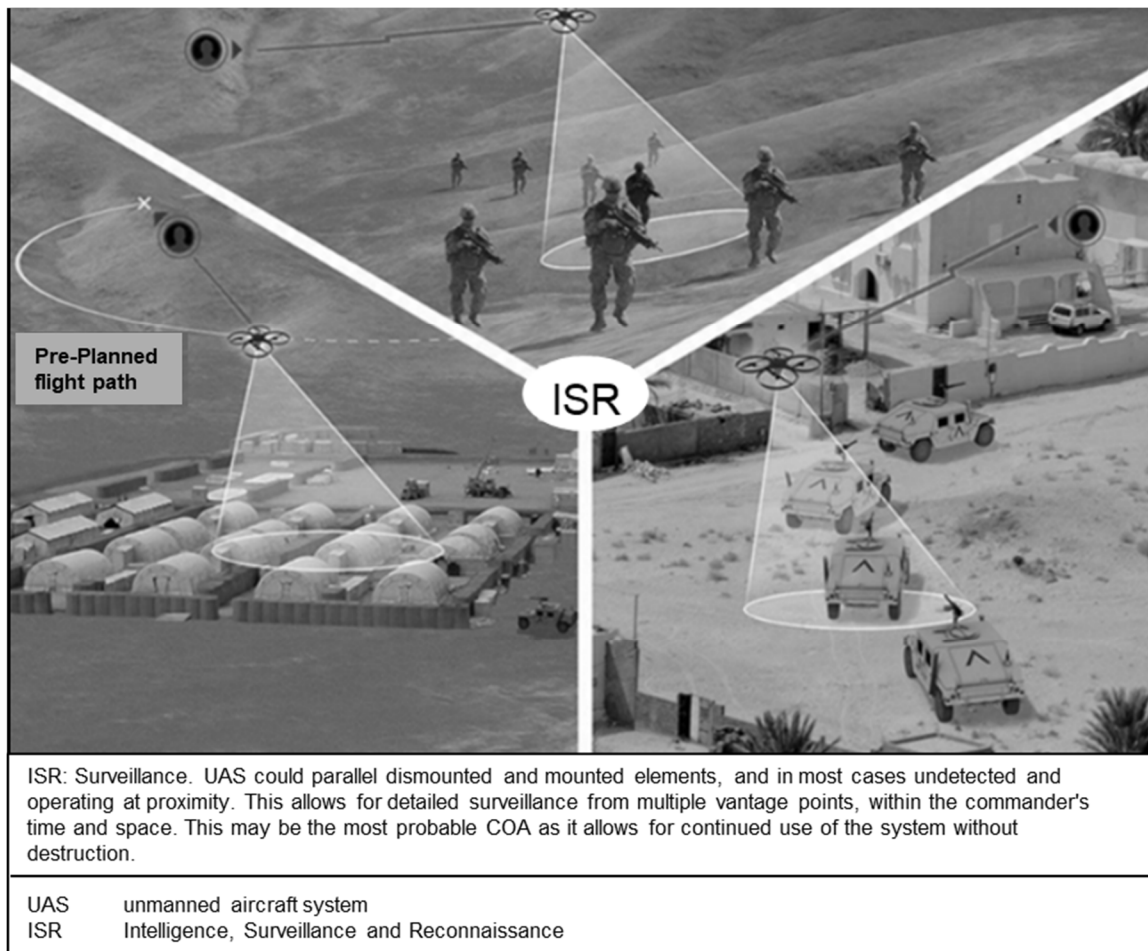


Figure 3-1. Unmanned aircraft system intelligence surveillance reconnaissance role

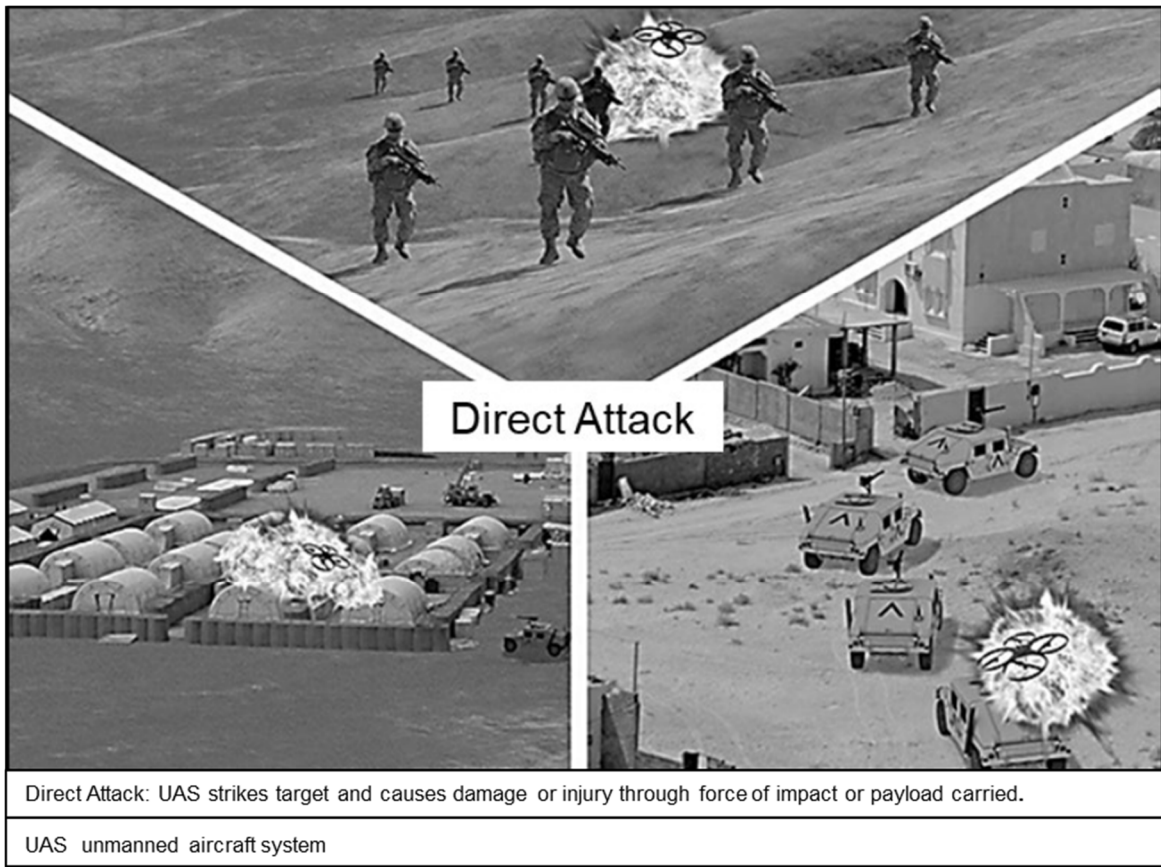


Figure 3-2. Unmanned aircraft system direct attack

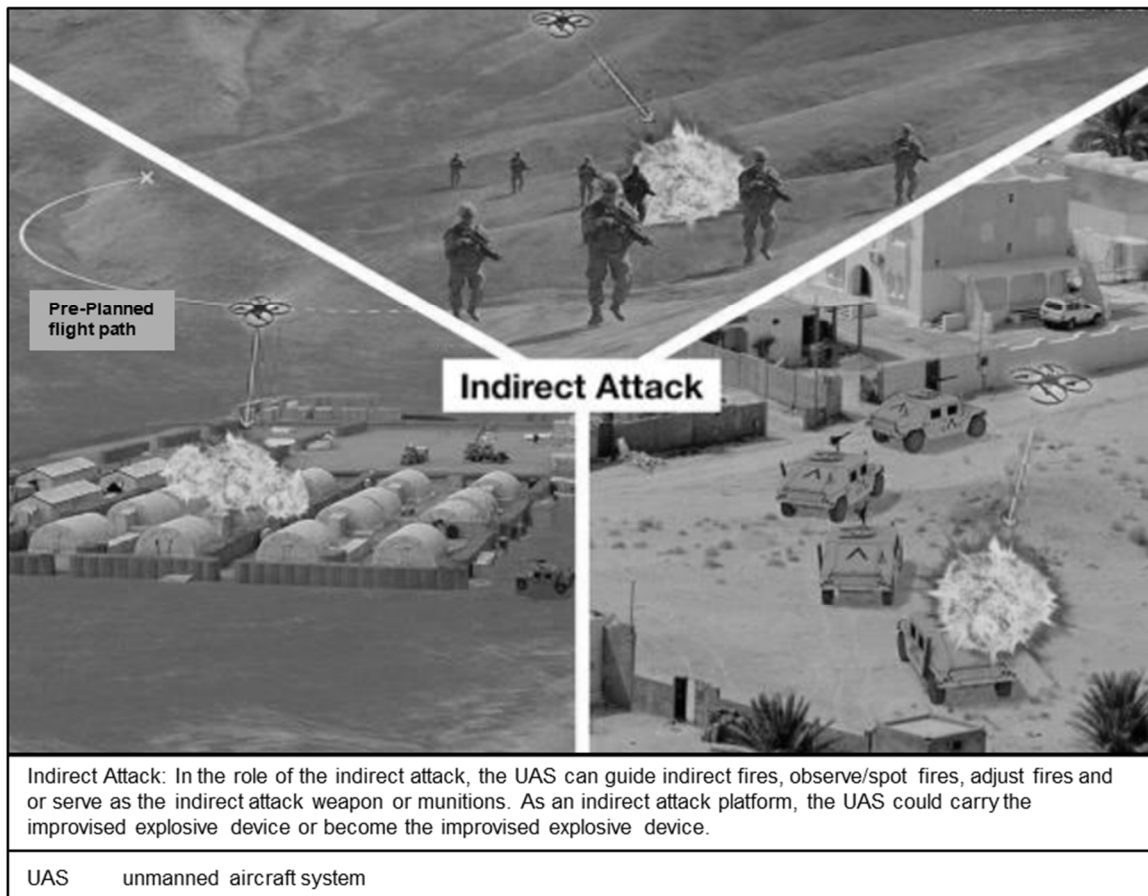


Figure 3-3. Unmanned aircraft system indirect attack

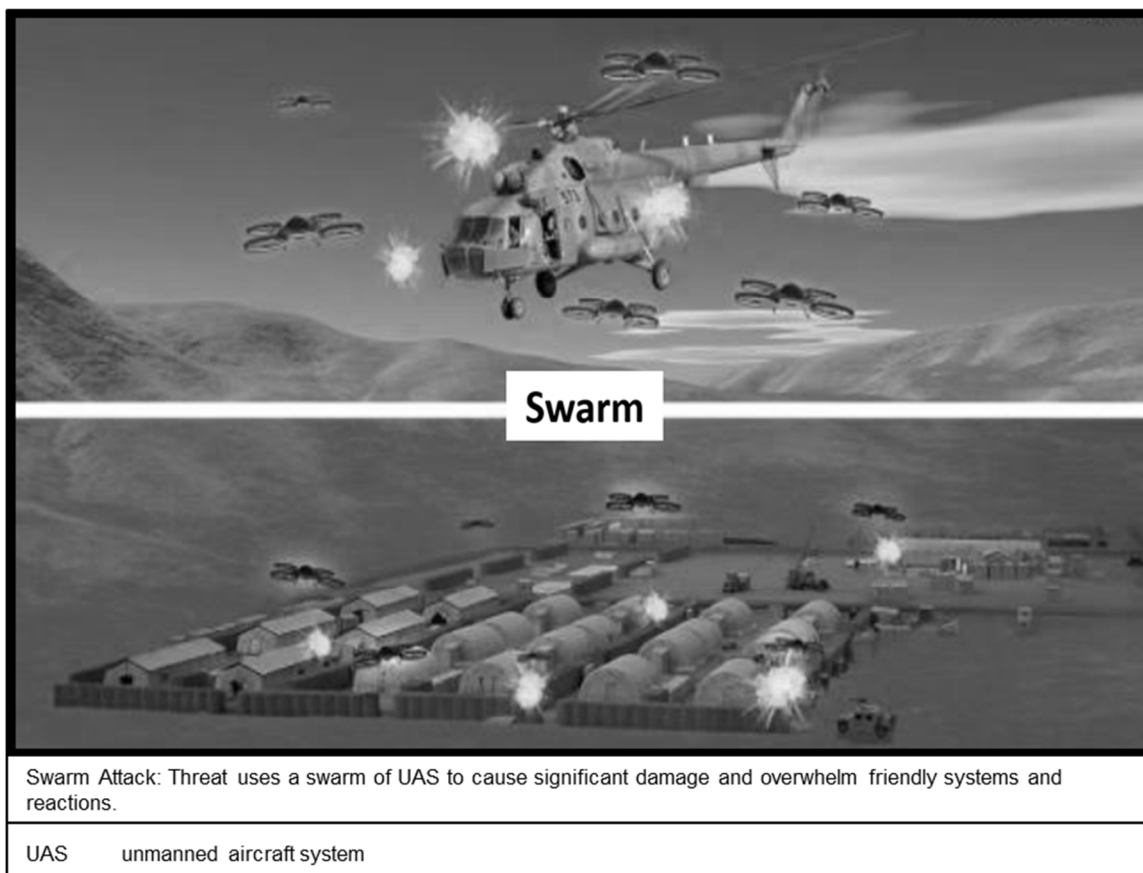


Figure 3-4. Swarm attack

3-3. Units operating in and around combat areas should assume the enemy is observing or attempting to observe them. Modern, friendly, and allied sensors, which include a host of robust long-range and short-range radars, optical devices, and audible alert systems, face challenges detecting the UAS Groups 1, 2, and 3 at sufficient ranges to mitigate effects. Threat UAS may go undetected while operating at a standoff range. ADA units cannot engage all hostile air threats, due to the lack of availability of ADA weapons and sensors, and/or equipment capability limitations. Such being the case, all units should be trained and ready to detect, identify and be prepared to engage UAS Groups 1 through 3.

3-4. Contact with unidentified UAS may be a precursor to an imminent attack. However, not all unidentified UAS encounters pose a risk. All units must react quickly and appropriately respond and report when recognizing signs of possible enemy observation or attack. Whether a counter-response capability is available or not, units must implement passive or active defense measures to nullify or reduce the effectiveness of enemy UAS operations.

COUNTERING THE THREAT

3-5. Countering the UAS threat requires a combined arms approach that leverages capabilities across many disciplines. Commanders must consider a wide range of capabilities to counter the UAS threat including active measures from direct fires, EW, and aviation as well as passive survivability and protection measures. Examples of contributions for countering UAS threats across the combined arms force include:

- Fires forces-
 - Integrate surveillance capabilities.
 - Identify targets.
 - Facilitate and conduct engagements.
 - Employ EA and/or kinetic capabilities to defeat or destroy UAS threats.
 - Support direct action against threat elements to prevent UAS threats prior to launch.

- Protection elements assist commanders to-
 - Identify critical capabilities, areas, information and prioritize protection resources.
 - Integrate cover, concealment, and deception (CCD) and C-UAS capabilities to build a layered defense.
 - Employ electromagnetic protection (EP) capabilities to protect critical networks and systems.
- Intelligence forces-
 - Identify UAS threat capabilities and associated tactics.
 - Collect and analyze threat sustainment networks to enable direct action against UAS systems, logistics and manufacturing/test facilities prior to launch.
 - Conduct exploitation activities to gain critical intelligence from captured threat UAS.
 - Conduct electromagnetic support to exploit UAS information gathered from the electromagnetic spectrum (EMS) and employ EA capabilities to defeat or destroy UAS threats.
- Maneuver forces-
 - Contribute to surveillance and identification of UAS threats.
 - Conduct direct action engagements of threat systems employing ground and aviation assets.
 - Employ EA capabilities to defeat or destroy UAS threats.
 - Conduct established recovery procedures to safely recover threat UAS for exploitation.
 - Employ survivability and protection measures across their formations.
- Command and control used to-
 - Integrate capabilities to enhance situational awareness and understanding.
 - Synchronize and converge all elements of combat power required to combat UAS threats at echelon.
 - Enable decision-making.

Chapter 4

Planning

This chapter describes the planning considerations and integration efforts needed to seamlessly incorporate and react during C-UAS operations into the overarching layered defense respective to the AMD mission set. Planning to defeat or mitigate impacts of threat, UAS must be included as part of an overall protection plan. Protection planning occurs as a holistic analysis of all threats, hazards, vulnerabilities, and criticalities. Commanders at the company and battery level must consider most likely threats, hazards, and the commander's protection priorities.

PLANNING CONSIDERATIONS

4-1. Countering the UAS threat can be accomplished through a combination of individual Soldier actions and survivability activities, blended with employment of equipment and systems ranging from organic weapons, to specialized handheld EW and lethal devices, to complex systems designed specifically to detect, identify, and defeat UAS. Many units may not be equipped with equipment designed specifically to counter the threat. Countering the threat may not focus solely on defeating the threat UAS; much of the activities to counter the threat may center on the mitigation efforts to lesson or eliminate the impact of a UAS mission against U.S. forces. These efforts should be conducted as part of a unit's overall protection and not as a standalone C-UAS plans and activities.

4-2. Planning is the first step toward effectively countering UAS threats. Combating the UAS threat requires a combined arms approach that leverages capabilities from all the warfighting functions. Combined arms operations use the capabilities of each function, along with leadership and information, in complementary and reinforcing capabilities (ADP 3-0). Planning effective actions to counter the UAS threat must synchronize activities across all the warfighting functions to ensure complementary and redundant capabilities executed as part of a holistic, layered plan (see figure 4-1 on page 22).

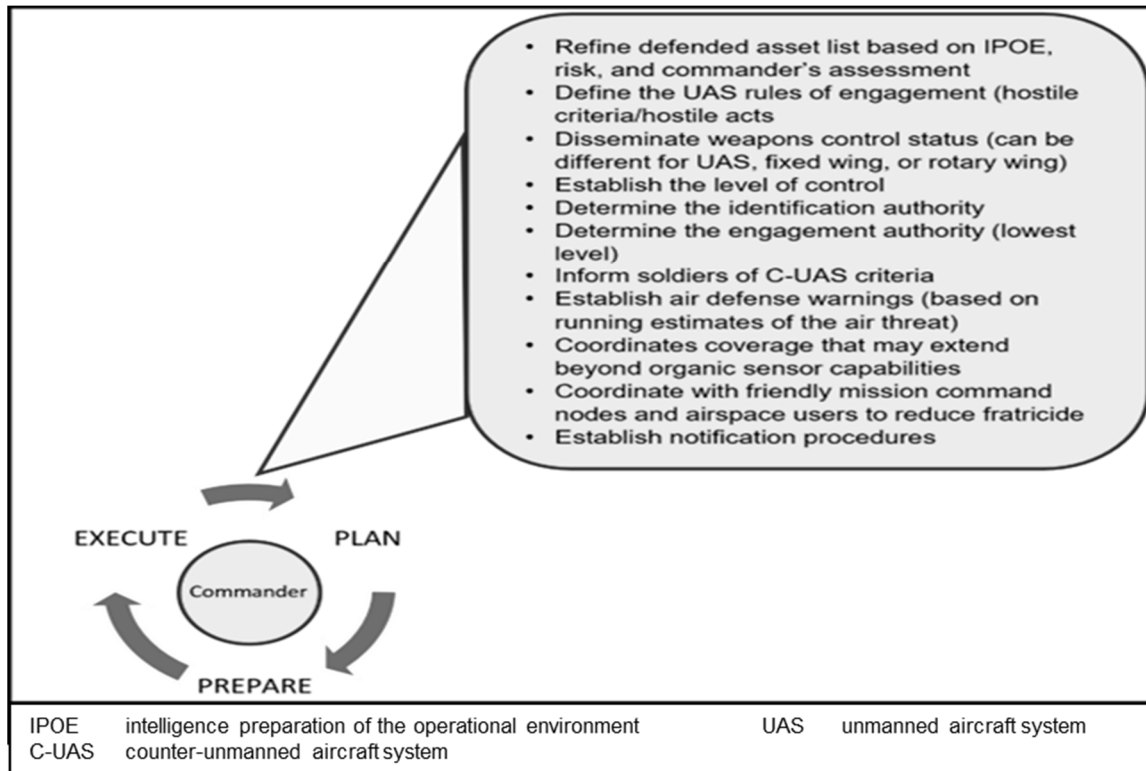


Figure 4-1. C-UAS planning considerations

4-3. The challenge for commanders at all levels is integrating available resources during the planning process to ensure their effective utilization during mission execution. Some systems are available that are specifically designed and/or optimized to address the UAS threat. These systems are employed based on their own unique capabilities to counter UAS threats. While specialized systems exist, commanders and planners must understand the UAS threat is not a singular problem requiring its own processes and solutions. The UAS threat is one of many threats that commanders face. Many of the actions used to mitigate the UAS threat are the same actions used to mitigate other threats and may already be employed. Commanders and leaders should employ basic planning methods and concepts, including the military decision-making process and troop leading procedures, integrating the UAS threat into the overall analysis and threat mitigation efforts.

4-4. Commanders have the responsibility to understand the ROE in order to take the appropriate actions to protect their forces. Planning and understanding the six AMD ROE categories (chapter 5) will aid in the protection of forces and equipment. The ROE do not inhibit commanders at all echelons from exercising the inherent right of self-defense to protect their forces from UAS. Commanders should note that advancements in commercial-off-the-shelf technology continue to present challenges at all levels for planners of C-UAS operations.

4-5. Planning for C-UAS activities should be part of a holistic protection planning effort. Successful efforts involve the tailored selection and application of multilayered active and passive measures commensurate with the level of risk. Countering UAS threats includes:

- *Active defense.* The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy (JP 3-60). It includes all direct defensive actions taken to destroy, nullify, or reduce the effectiveness of hostile threats against friendly forces and assets. (See chapter 5 for more information on active defense.)
- *Passive defense.* A measure taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative (JP 3-60). It includes measures, other than active defense, to minimize, mitigate, or recover from the consequences of threats against friendly forces and assets. These measures include camouflage, concealment, deception, dispersion,

reconstitution, redundancy, detection and warning systems, and the use of protective construction. (See chapter 5 for more information on passive defense.)

ASSESSMENT AND REPORTING

4-6. Planning occurs as a holistic analysis of all threats, hazards, vulnerabilities, and criticalities. Commanders and staff must consider-

- Most likely threats and hazards.
- Protection priorities.
- Which personnel, physical assets, and information to protect.

4-7. Commanders and staff must address C-UAS relevant areas within the protection planning process. Initial planning requires various assessments to establish protection priorities including-

- Criticality assessments.
- Vulnerability assessments.
- Threat assessments.
- Hazard assessments.

ASSESSMENT CATEGORIES

4-8. Initial protection planning requires various assessments to establish protection priorities. These assessments include criticality assessments, vulnerability assessments, and threat and hazard assessments. During these assessments commanders and staff must ensure C-UAS relevant areas are addressed.

4-9. A criticality assessment identifies key assets that are required to accomplish a mission:

- It addresses the impact of a temporary or permanent loss of key assets or the unit's ability to conduct a mission.
- It should also include high-population facilities (recreational centers, theaters, sports venues) that may not be mission essential.
- The general sequence for a threat assessment is-
 - Assess the probability an asset will be targeted for surveillance or attack by a credible/capable adversary.
 - Determine likely adversary intent and capability which are key determinants of assessing the probability of attack.
 - Utilize the intelligence preparation of the operational environment (IPOE) process to estimate adversary capabilities.

4-10. A vulnerability assessment is an evaluation to determine the magnitude of a threat's or hazard's effect on an installation, personnel, a unit, an exercise, a port, a ship, a residence, a facility, or other site.

- The vulnerability assessment determines an asset's susceptibility or the degree to which an asset is susceptible to surveillance, attack or damage.
- The vulnerability assessment also addresses recoverability of an asset, if the asset is attacked and damaged; this assists in determining the degree of potential damage and ability to recover/reconstitute from inflicted damage in terms of time, equipment, and manpower and to continue the mission. The general sequence of a vulnerability assessment is:
 - List assets and capabilities and the threats against them.
 - Determine the common criteria for assessing vulnerabilities.
 - Evaluate the vulnerability of assets and capabilities.

4-11. Threat and hazard analysis comprises a thorough, in-depth compilation and examination of information and intelligence that addresses potential threats and hazards. During threat and hazard analysis commanders and staffs must ensure-

- UAS threats are included: actors, entities, or forces that have the capability and intent to harm U.S. forces, U.S. national interests, or the homeland are considered threats.
- Potential hazards from threat UAS are identified; a threat is a condition with the potential to cause injury, illness, or death of personnel; damage to or loss of equipment or property; or mission degradation. The general sequence for a threat and hazard assessment is:

- Assess the probability an asset will be targeted for surveillance or attack by a credible/capable adversary.
- Determine likely adversary intent and capability which are key determinants of assessing the probability of attack.
- Utilize the IPOE process to estimate adversary capabilities.

4-12. Analysis of the results of criticality assessments, vulnerability assessments, and threat and hazard assessments feed into the protection priority list. All assets nominated for the protection priority list are usually prioritized based on a methodology of assessing the three major factors of criticality, vulnerability, and threat. The criticality, vulnerability, and threat process are subjective and considers intelligence, air operations, ground combat operations, support operations, and host nation (HN) considerations. Each asset is evaluated against defined criteria, and these criteria are weighed based commander's priorities and intent.

REPORTING

4-13. Units must set conditions allowing forces at all echelons, to recognize and report airspace violations and confirmed enemy actions that occur within their AO. Planners must include current threat sets and standardized reporting guidance. See table 4-1 for an example of a standardized spot report for reporting initial contact. Theater specific reports may vary based on command directive, mission and environmental requirements. This information should include its description and flight profile.

4-14. A unit's standard operating procedures may also include model and capability profiles for known threat UAS. These profiles will provide C-UAS planners the suite of capabilities associated with the threat. Flight profiles associated with a threat UAS can assist unit C-UAS planners in planning for a specific UAS threat. This will assist in conducting unit-specific C-UAS tactics, techniques, and procedures (TTP).

4-15. Detecting threat UAS by organic sensors or through observation can assist in determining its model and flight path. Calculating speed and heading and knowing the UAS's endurance, based on flight profiles, improves a unit's chance of mitigating the UAS ability to conduct ISR and execute attacks on friendly forces. While sensors may detect many of the larger UAS, it is likely that unit air guard may be the primary detection means for UAS. Air guard must be familiar with UAS capabilities and be able to recognize behaviors and patterns. Air guard must provide continuous updates, through reports to unit operations personnel, to develop an evolving defense against threat UAS.

4-16. Soldiers must train to report contact as soon as possible following detection of a UAS operating in the area. The size, activity, location, unit, time, and equipment (known as SALUTE) acronym/format can be used to immediately generate and deliver a spot report to the chain of command (see table 4-1). The chain of command will then determine what immediate actions need to be taken and will generate required follow-on contact reports.

Note. The SALUTE format is intended to be a starting point in the reporting structure. It is not meant to take the place of any local/command mandated report format. This is a baseline format for personnel to report first contact; upon receipt this report should trigger follow-on information collection and security actions as required.

Table 4-1. Standardized Counter- Unmanned Aircraft System Detection Report Example (SALUTE Format)

<i>Line</i>	<i>Information</i>	<i>Example</i>
1	Size	Report the number of UAS, or size of the formation (e.g., single, multiple, or swarm).
2	Activity	Report detailed account of actions: What is the direction of movement? Was there any hostile action? Is the threat UAS loitering in one spot (possibly has spotted reporting unit)? Is it flying straight (enroute to loitering location)? Was the threat UAS approach observed or was it spotted overhead?
3	Location	Report where you saw the activity. Include 6 to 8 digit grid coordinate of reporting element, grid or distance and direction from reporting element location (known point).
4	Unit (Description of UAS)	Report fixed-wing or multi-rotor, wingspan, height, color, tail configuration, rotor configuration, lights, other distinguishable markings.
5	Time	Report the time the activity was observed, not the time you report it. Annotate it in either local or Zulu time. (Example: Date-time group: 091024ZMAR18)
6	Equipment	Report all equipment associated with the activity, such as payload, weapons, and camera.
UAS Unmanned Aircraft System		

PLANNING AND PREPARING COMPONENTS

4-17. Commanders utilize the operations process to drive the conceptual and detailed planning necessary in order to better understand the OE. This allows them the ability to visualize and describe the operations end state and operational approach; make and articulate decisions; and direct, lead, and assess military operations. The major command and control activities performed during operations are planning, preparing, executing, and continuously assessing the operation (ADP 5-0). Table 4-2 on page 26 depicts the relationship between framework components, the operational phase, and the desired end state related to—

- Deterrence: (Pre-Incident)
 - Shape OE through policy, influence activities, and understanding of civilian UAS manufacture geofence software.
 - Prevent or limit neutral or non-combatant UAS in the OE.
 - Limit enemy UAS procurement, distribution and employment networks.
- Preparation: (Pre-Incident)
 - Identify enemy UAS TTP, payload capabilities, and methods of UAS control, expected number of UAS in the OE, flight profiles, and evasion capability.
 - Develop TTPs for detection, response, site exploitation, and reporting based on the IPOE and potential enemy UAS activity.
 - Implement ROE and rules of use of force for UAS, focused with a proportionate response to avoid premature forced evolution of enemy TTPs.
 - Conduct UAS battle drills based on enemy UAS capabilities, ROE/rules for the use of force, and C-UAS capabilities for fixed and dismounted scenarios.
 - Conduct spectrum coordination and deconfliction with friendly actors in the OE.
 - Analyze and understand the impact friendly C-UAS capabilities will have on other friendly assets operating in the spectrum.
 - Format standardized, disseminated, and rehearsed reports for C-UAS.
 - Train and rehearse for C-UAS responses.
 - Identify potential launch sites and controller locations
- Detection:
 - Identify enemy UAS as early as possible.
 - Send hasty initial report of UAS sighting.
 - Conduct C-UAS response informed by IPOE and preparation.

- Response: (trans-incident)
 - Secure the site of a UAS incident in coordination with tempo of land operations.
 - Conduct UAS retrieval in accordance with unit TTP developed in the preparation component.
 - Maintain security of enemy UAS and submit to appropriate lab for analysis.
- Report: (post-incident)
 - Submit full report in accordance with unit standard operating procedure.
- Synthesis: (post-incident)
 - Leverage intelligence obtained from a UAS incident to inform potential methods of deterrence and engagement, thus enhancing C-UAS actions against future attacks.
 - Use intelligence obtained from UAS incident to strengthen preparation for future C-UAS operations.

Table 4-2. Framework components

Framework	Operational Phase	End State
Deterrence	Plan/Prepare	Enemy dissuaded from employing UAS
Preparation		Understand the OE, threat, TTPs, and countermeasures
Detection		Enemy UAS identified at the earliest opportunity
Response	Execute	Neutralize or evade the enemy threat
Site exploitation	Assess	Enemy UAS rendered safe and information extracted
Reports		Timely, detailed incident report submitted
Synthesis		Incident drives adaptive response to future incidents
OE operational environment	UAS unmanned aircraft system	TTPs tactics, techniques, and procedures

4-18. *Risk management* is the process to identify, assess, and mitigate risks and make decisions that balance risk and cost with mission benefits (JP 3-0). The C-UAS planning process assists commanders in making informed decisions to balance risk with mission benefits. The process itself evaluates the threat problem, collateral concerns, environment or medical hazards, impacts to capabilities, risk to force, and risk to mission, before or during execution of actions. (See ATP 5-19 for additional information on risk management.)

PLANNING RESPONSIBILITIES

4-19. Brigade and higher headquarters are responsible for the integration of C-UAS into military decision-making process and working groups to include targeting and protection processes. In addition, the ADAM/BAE and EW officer will manage the airspace and C-UAS sites and mobile systems' employment. The C-UAS fight requires a multi-echelon approach, synchronizing resources of higher echelons to support mitigation of the tactical UAS threat. Brigade and lower echelons execute protection and survivability activities to mitigate UAS threats on their positions and conduct direct engagement of immediate UAS threats (in flight).

4-20. Higher echelons conduct analysis and planning to mitigate the UAS threat and direct resources to enhance survivability of subordinate friendly forces. They direct resources to ensure U.S. forces and our allies maintain a real-time common operating picture relevant to the UAS threat and identify UAS production and associated sustainment resources used by threat elements. These activities may lead commands above brigade level to direct and coordinate direct action against those threats when required. Actions against large UAS platforms are conducted at echelons leveraging joint capabilities.

4-21. Division and brigade-level ADA/EW staffs should advise lower echelons with respect to integration of planning C-UAS activities into their military decision-making, targeting, and protection processes.

4-22. Company-level mission command requires an understanding of the tasks relative to C-UAS operations using a quick reference guide or pre-combat checklist. Company will be responsible for the employment of the handheld equipment to detect and/or defeat Group 1 UAS. Company-level security operations will be

enhanced by integrating air guards into their security planning. Platoon leaders conduct rehearsals to plan air guard tasks, locations, UAS spot report procedures, and communication plans. Soldiers will incorporate air guard principles into existing search and scan techniques throughout all phases of the operation. (See Chapter 4 for more details.)

ELECTROMAGNETIC WARFARE CONSIDERATIONS

4-23. *Electromagnetic warfare* is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy (JP 3-85). The Army continues to build EW competencies to support decisive action and win across all levels of combat operations and throughout all domains. Leaders must consider EA, EP, and ES capabilities when planning for counter-small unmanned aircraft system operations.

4-24. *Electromagnetic attack* is the division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires (JP 3-85). EA has the unique potential to affect enemy use of the EMS and attack the enemy through the EMS. Various capabilities can be used to destroy, degrade, disrupt, and deceive the threat's military EMS actions. Once the commander's intent is understood, the CEMA section, in coordination with the staff, should carefully consider the following-

- Interference with friendly communications.
- Intelligence gain or loss.
- Spectrum use by neutral actors.
- The persistence of effects.
- Electromagnetic signatures.
- Personnel and equipment capabilities and limitations.
- Persistency of effect: Effects of jamming only persist as long as jammer itself is emitting and is in range to affect the target.

4-25. *Electromagnetic protection* is the division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability (JP 3-85). EP includes actions taken to ensure friendly use of the EMS, such as frequency agility in a radio or variable pulse repetition frequency in radar. EP is essential to prevent the adversary from learning behavior and intentions within the EMS. EP techniques that should be considered include:

- Spectrum management.
- Electromagnetic hardening.
- Electromagnetic masking.
- Emission control.
- Electromagnetic compatibility.
- Terrain masking.
- Wartime reserve modes.

Note. Refer to ATP 3-12.3 for more information on EP.

4-26. *Electromagnetic support* is the division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations (JP 3-85). Electromagnetic support gathers information about friendly and threat electromagnetic emissions to support the commander's situational awareness and decision making. ES is accomplished through the following tasks:

- Electromagnetic reconnaissance.
- Threat warning.
- Direction finding.

Note. Refer to ATP 3-12.3 for more information on ES.

4-27. *Electromagnetic interference* is any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment (JP 3-85). Electromagnetic interference prevents successful EM transmissions; units must recognize and mitigate electromagnetic interference to create the conditions required to use the EMS to communicate.

C-UAS AND THE ARMY TARGETING PROCESS

4-28. While there is no specific doctrine delineating UAS targeting, C-UAS operations follow the Army targeting process using the decide, detect, delivery, and assess methodology. C-UAS will still fall under dynamic or deliberate targeting categories and the methodology will remain the same. Decide, detect, deliver, and assess methodology organizes the efforts of the commander and staff to accomplish key targeting requirements.

4-29. Targeting is an outgrowth of the commander's decisions and establishes the requirements for the development of an effective information collection effort. It helps the staff and targeting working group decide which targets need to be acquired and engaged. Targeting working groups can vary in make-up and size as determined by the commander and standard operating procedures of the unit. C-UAS operations will be nested in the joint targeting process when division level echelons need C-UAS solutions. Joint targeting will follow a similar targeting cycle for UAS threat sets. Refer to JP 3-60 for more information regarding joint targeting doctrine.

LAYERED DEFENSE

4-30. Commanders and staff must plan for defense in depth, employing successive layers of C-UAS capability to overlap area and local defense asset coverage areas and mitigate dead spaces. The unit should develop and refine C-UAS 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.

4-31. Commanders, staffs, and Soldiers execute C-UAS activities as part of an overall protection plan employing the five principles of protection: comprehensive, integrated, layered, redundant, and enduring. (Figure 3-1).

- Comprehensive-Protection is an all-inclusive utilization of complementary and reinforcing protection tasks and systems available to commanders and incorporated into the plan to preserve the force.
- 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 range of military operations. Integration must occur vertically and horizontally with unified action partners throughout the operations process.
- Layered-Protection capabilities are deliberately sequenced across multiple domains to eliminate, mitigate, or assume the risk of threat effects.
- Redundant-Protection efforts for identified critical vulnerabilities require dedicated primary and alternate protection capabilities.
- Enduring-Protection is a continuous activity. Commanders and leaders preserve combat power and reduce the risk of loss, damage, or injury to their formations.

4-32. Seven ADA employment tenets tie directly into layered defense and optimum protection from UAS. They are mutual support, overlapping fires and overlapping coverage, balanced fires, weighted coverage, early engagement, defense in depth, and resilience.

- Mutual Support. Weapons are positioned so that the fires of one weapon can engage targets within the dead zone of the adjacent weapon. For guns, this dead zone is usually small. For missiles, the dead zone may be large, and mutual support is a critical element. Mutual support can also cover nonoperational weapons or weapons at lower states of readiness. Mutual support, when applied to

sensors has the same connotation; that is, sensors are deployed to cover the dead zone of adjacent sensors.

- **Overlapping Fires and Overlapping Coverage.** Weapons are positioned so that their engagement envelopes overlap. Because of the many altitudes, directions, and ranges from which the enemy can attack or conduct surveillance operations, defense planners must apply mutual supporting and overlapping fires vertically and horizontally. Overlapping coverage is the positioning of sensors such that their coverage does not leave any seam in the defense that might be used by incoming threats. Overlapping fires and overlapping coverage should be planned during defense design.
- **Balanced Fires.** Weapons are positioned to deliver an equal volume of fires in all directions. This is necessary for AMD in an area where the terrain does not canalize the threat or when the avenues of approach are unpredictable. Balanced fires are a desired characteristic of defense design against cruise missiles and other air threats.
- **Weighted Coverage.** Weapons coverage is combined and concentrated toward the most likely threat air avenues of approach or directions of attack. Based on the tactical situation, a commander may risk leaving one direction of attack unprotected or lightly protected to weight coverage toward another direction. Weighted coverage and balanced fires are not mutually achievable, requiring the defense designer to give up most aspects of one to achieve the other.
- **Early Engagement.** Early engagement generally requires extending the defense away from the defended asset. Sensors and weapons are positioned so they can engage the threat before ordnance release or detection of friendly forces. Early engagements enable destruction of enemy platforms over enemy forces and unoccupied areas, thereby reducing the possibility of friendly collateral damage and fratricide. As with weighted coverage, early engagement is achieved at the expense of balanced fires.
- **Defense in Depth.** Sensors and weapons are positioned so that the threat is exposed to a continuously increasing volume of fire as it approaches the friendly protected asset or force. Defense in depth decreases the probability that attacking missiles, aircraft, or RAM will reach the defended asset or force.
- **Resilience.** Resilience is the quality of the defense to maintain continuity of operations regardless of changes in or unanticipated tactics by enemy air or losses of critical air and missile defense components (FM 3-01). ADA planners must plan for defense design adjustment based on ADA system attrition. Resilience is a key determinant when considering which tenet (or tenets) to use in maintaining the defense.

4-33. Applying these principles increases capability density as a threat approaches the inner ring of defense. A UAS is faced with layered, collocated or integrated systems; increased sensor coverage; and no seams in the area or local defense (all dead spaces are covered). Layering protection capabilities enables commanders and staffs to deliberately sequence capabilities and mitigation measures across multiple domains to eliminate, mitigate, or assume the risk of threat effects. (See chapter 5 for additional discussion of both active and passive measures in a layered defense.)

- Layer area and local defense assets.
- Coverage increases as the UAS approaches.
- Ensure dead space coverage.
- Co-locate or integrate systems.

LAYERED DEFENSE TECHNIQUES

4-34. A layered defense approach provides strength and depth. Units use their available capabilities to defend personnel and critical assets through layering of capabilities to prevent threat UAS attacks. When the threat cannot be stopped, techniques are applied to reduce the destructive effect of threats and hazards. Individuals are protected at the lowest level by awareness, personal protective equipment, an understanding of the ROE, and fratricide avoidance measures. Additional protection measures are implemented in the surrounding area such as fighting positions, observation posts, and equipment with specific protection capabilities to achieve layered collective protection. Techniques employed by all Soldiers, application of well-planned and executed survivability measures, coupled with application of C-UAS capabilities employed in depth and mutually supporting, are critical to the overall C-UAS effort. See Figure 4-2.

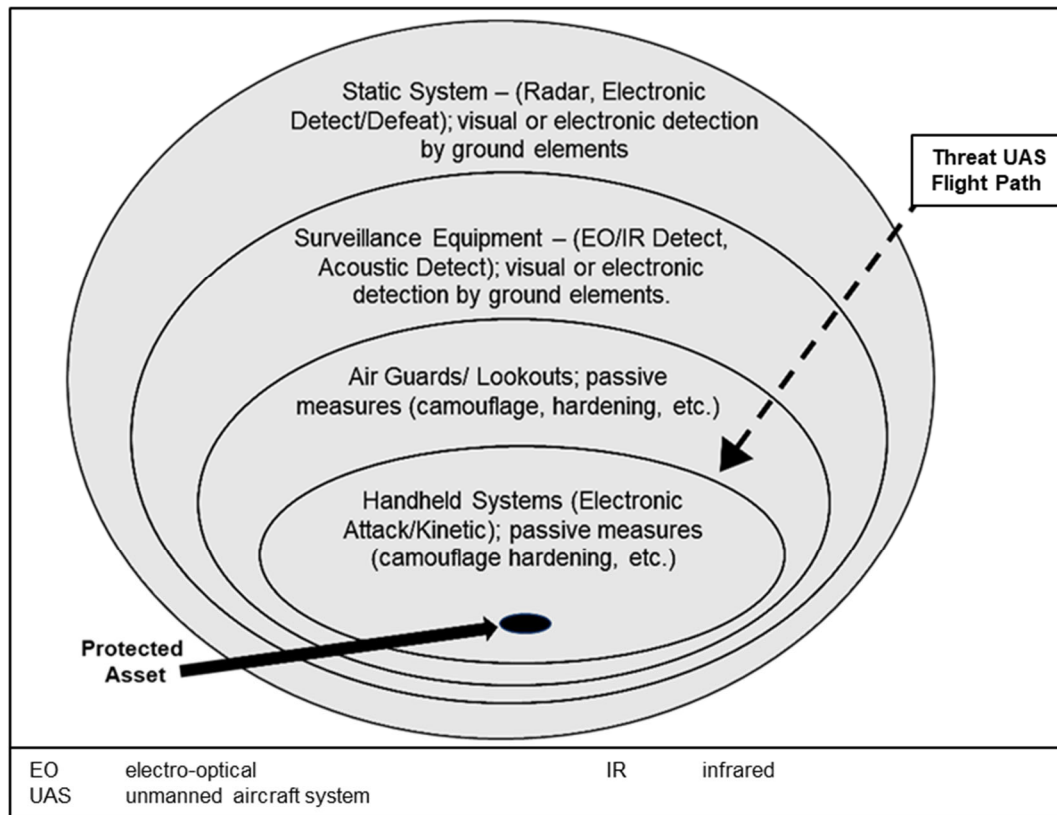


Figure 4-2. Layered defense unmanned aircraft system example

4-35. Commanders, leaders and planners must include the simultaneous application of both passive and active measures during operational planning and employment as part of a layered defense strategy against UAS threats. Leaders must understand active measures help deny the initiative to the enemy or adversary, while the execution of passive defense measures prepares the force against threat and hazard effects and accelerates the mitigation of those effects. (See chapter 5 for more information on passive and active measures.) Key tasks to integrate into plans and combined arms unit training strategies addressing UAS threats are:

- Identify critical assets to be protected.
- Perform cover and concealment.
- Harden unit positions.
- Employ dedicated air guards.
- Perform visual aircraft recognition training.
- Conduct air threat avoidance techniques.
- Conduct deception/decoys and dispersion techniques.
- Establish a security force and quick reaction force.
- Establish an organic early warning sensor network.
- Conduct UAS reporting procedures.
- Conduct downed UAS recovery/battle damage assessment.
- Select UAS defeat mechanisms.
- Perform unit recovery and reconstitution.
- Disseminate UAS threat warning and response option readiness levels.
- Coordinate threat representative UAS red team flights for system operational readiness and training purposes.
- Understand and employ C-UAS systems to maximize range and effectiveness.

- Employ multiple capabilities to provide redundancy, mutual support, and complementary capabilities in depth.
- Determine likely launch sites and controller locations relative to friendly operations in time and space.

4-36. Units may be equipped with systems designed specifically to defeat UAS threats. These systems may be employed by an individual, may be employed by a small team of two or three personnel, may be carried to provide coverage over a dismounted element, may be mounted on vehicles, or they may be complex system-of-system with capabilities requiring specialized training and crew certification. When employing these systems commanders and leaders should consider—

- Threat:
 - Identify and understand all potential threat UAS for the area of operations.
 - Identify and understand common enemy TTP.
- Site selection. The following is a list of criteria involved in site selection:
 - Line of Sight (LOS). Many systems require LOS to a target. Analyze terrain to identify dead spaces and determine coverage strategies. LOS verification can be accomplished through use of 3D mapping tools and visual LOS analysis.
 - Multiple systems should be employed to ensure no dead zones.
 - Systems are emplaced to maximize LOS.
- Background electromagnetic environment (known as EME). System placement in areas of high electromagnetic density can create a masking effect, preventing UAS detection. Analyze terrain to ensure optimum placement of sensors to reduce signal disruption. Ensure that all C-UAS EW plans and operations are integrated. Consider adjacent equipment compatibility and effects of background EME for the following:
 - Radars.
 - Communications equipment.
 - Counter improvised explosive device/EW equipment.
 - Wi-Fi networks.
 - Other wireless systems.
- Priorities for protection.
 - Identify commander's critical assets for protection.
 - Focus defense based on priorities. Emplace assets to secure high priority assets first.
- Clearance of fires (for lethal capabilities).
- System limitations.
 - Range of the system (lethal and non-lethal).
 - Atmospheric and terrain effects.
 - Equipment optimization.
 - Jamming frequencies.
 - System library limitations.
 - Other radio frequency (RF) transmitting systems (vehicle Wi-Fi, remote control doors, etc.) that may appear as unmanned aircraft signal detections.
- For C-UAS systems site surveys, system validation, and employment, identify and consider leveraging-
 - ADA assets within the organic unit, higher echelons, and adjacent units.
 - EW assets within the organic unit, higher echelons, and adjacent units.
 - Available field service representatives.
 - Mobile training team support (when available).

4-37. Employing a successful fixed-site layered defense, or defense in depth, against the UAS threat requires layering area and local defense assets to ensure redundancy, mutual support, and complementary capabilities in depth. A layered defense ensures that coverage increases as the threat UAS approaches protected assets/areas (number and density of C-UAS assets increases as range to protected assets reduces). Leaders must ensure that dead space is covered through mutual support of systems and capabilities; this is accomplished through co-location and integration of complementary supporting systems and capabilities.

4-38. To plan and execute a successful layered defense strategy, commanders and staffs must first identify the critical assets being protected. It's accomplished through criticality assessments, vulnerability assessments, and threat and hazard assessments. The results of these assessments are the commander's protection priority list. This provides the prioritized list of assets to be defended.

4-39. Countering the threat is not focused on solely defeating the threat UAS; much of the activities to counter the threat are centered on mitigation efforts to lessen or eliminate the impact of a threat UAS mission against U.S. forces. These efforts are conducted as part of a unit's overall protection plan; they are not stand-alone counter UAS plans and activities. Countering the threat requires individual Soldier actions and survivability activities, blended with employment of equipment and systems ranging from organic weapons, to specialized handheld EW and lethal devices, to complex systems designed specifically to detect, identify, and defeat UAS. Not all units will be equipped with equipment designed specifically to counter the threat.

4-40. The first layer of defense includes all the individual Soldier skills and tasks required for personal protection and defense in the immediate area. Next, survivability tasks are employed to harden critical assets to mitigate the effects of an attack by UAS or other enemy capability. These tasks and activities protect against many risks present in the operational area not just UAS threats. These tasks and activities are conducted as part of a holistic protection plan (see table 4-3). Considerations and requirements include-

- Individual Soldier task proficiency.
- Trained proficiency in attack and emergency response battle drills.
- Survivability measures applied to critical assets.
 - Camouflage.
 - Cover and hardening.
 - Concealment (including techniques to hide, blend, obscuration or disrupt the outline).
- Use of decoys and deception to fool adversaries.
- Compartmentalization to mitigate threat impacts.
- Emplacing observation posts.
- Bunkers and fighting positions.
- Conducting combined arms for air defense.
- Conducting direct fire attacks against airborne assets.

Table 4-3. Survivability techniques

<i>Threat Sensor Systems</i>			
Friendly Techniques	Optical	Thermal	Radar
Hiding	Earth cover Earth embankments Vegetation Camouflage nets Screens obscuration	Earth cover Earth embankments Vegetation Camouflage nets Screens Obscuration	Chaff Earth cover Earth embankments Vegetation Nets Radar-absorbing material Camouflage nets
Blending	Paint Foam Lights Vegetation Camouflage nets Textured mats	Thermal paint Foam Air conditioning/heating Vegetation Camouflage nets Textured mats Water Insulation	Vegetation Camouflage nets Radar-absorbing material Reshaping Textured mats
Disguising	Reshaping Paint Camouflage nets	Reshaping Paint	Corner reflectors
Disrupting	Camouflage sails False operating surface Pyrotechnics Smudge pots Balloons Strobe lights Tracer simulators Obscuration	Flares Obscuration	Chaff Corner reflectors
Decoying	Decoy target (pneumatic or rigid structures) Lights Obscuration	Decoy target Flares Air conditioning/heating Obscuration	Decoy target Corner reflectors Signal generators

4-41. Commanders and leaders must identify where observation positions combined with multiple C-UAS capabilities and systems are emplaced in a layered and integrated manner to provide maximum protection from a threat UAS. A thorough terrain analysis should be conducted to determine lines of sight and associated dead space that must be accounted for in the overall plan.

4-42. When C-UAS systems with EW capability are present, a thorough analysis and survey of the area of operation should be conducted prior to system emplacement. Special emphasis should be placed on understanding the background EME of the AO and optimizing equipment for operation, ensuring systems have clear line of sight and are not placed in defilade or other areas that may affect RF propagation.

BUILDING THE DEFENSE FOR FIXED SITES

4-43. When building a defense in depth leaders must first identify and protect critical assets. This requires employing survivability techniques to protect these assets within the perimeter of the base of operation (see figure 4-3 on page 34). Additional survivability measures will be required if observation points and fighting positions are placed outside the base perimeter. Blast mitigation and stand-off should always be considered when employing survivability measures.

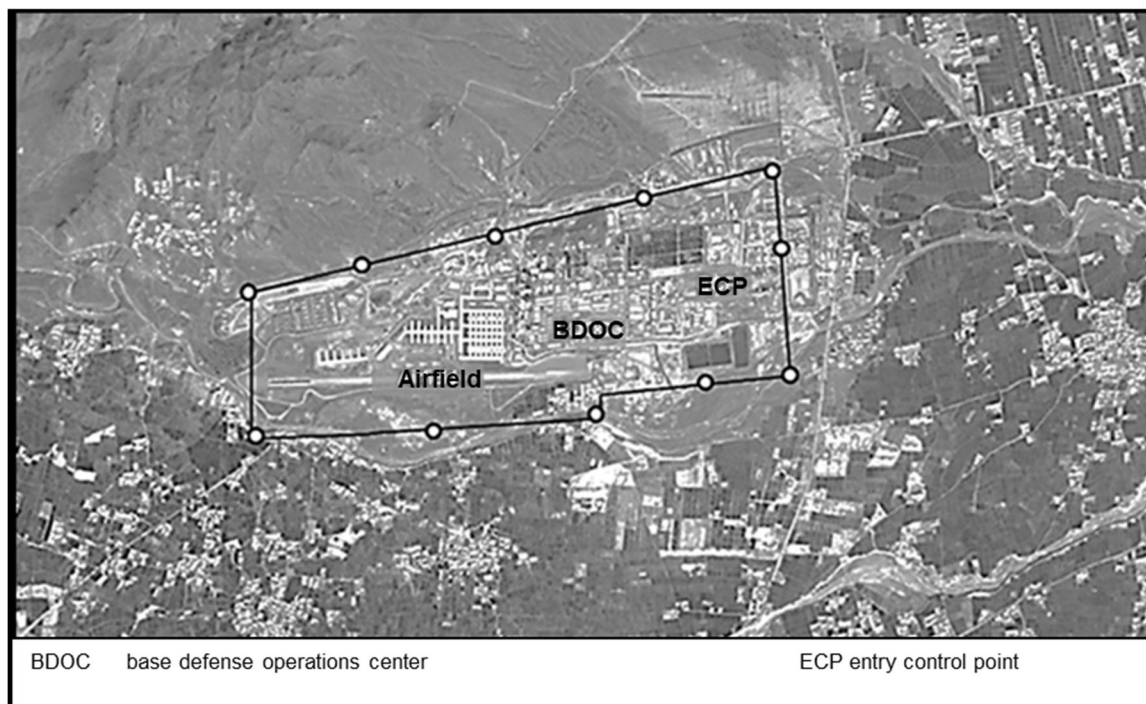


Figure 4-3. Fixed site

4-44. Once the maximum detect range is identified, the maximum defeat range must be established. The maximum defeat range will vary by system but must be identified in order to prevent threat UAS from completing its assigned task. Security forces positions (air guards/observation posts) should be identified and prepared to visually detect threat UAS during hours of day light and limited visibility. These positions should be placed to mitigate any potential dead space where detection equipment capabilities are limited (see figure 4-4).

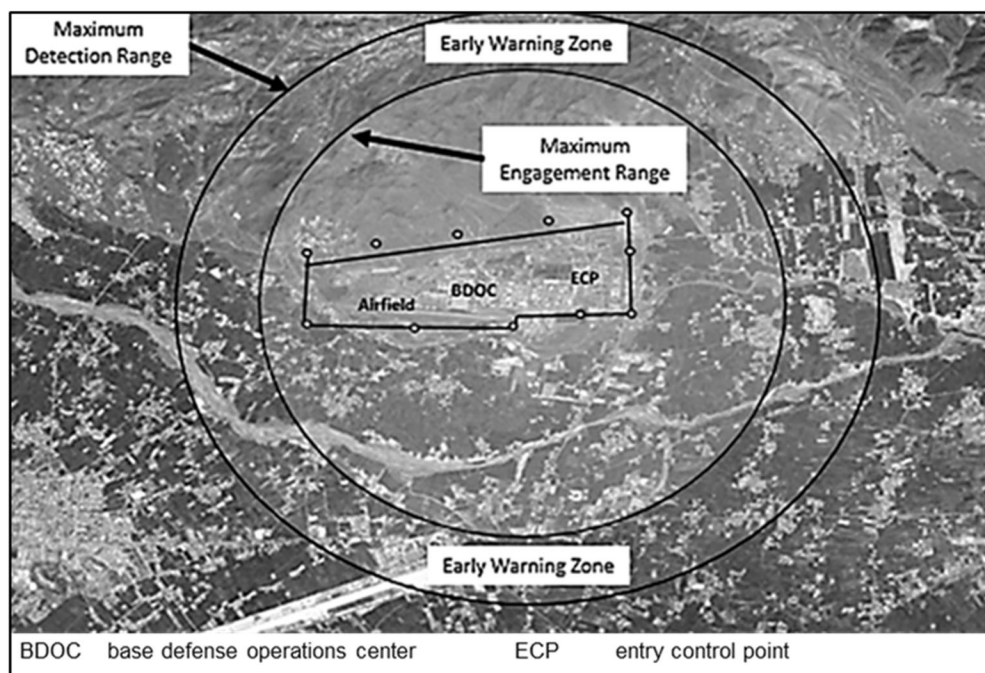


Figure 4-4. Detection and engagement ranges

4-45. If handheld or man-packed C-UAS systems are available, these can be distributed to observation posts to cover dead space or on critical avenues of approach (see figure 4-5). Leaders should consider emplacing these systems on elevated positions to prevent masking from terrain and structures. Commanders and leaders should consider emplacing some portable systems at static posts to defend critical assets. Others should be assigned to mobile elements to allow for response to any location on the site. Units may also be equipped with optical persistent surveillance systems. These systems are omnidirectional and can be slewed to give visual confirmation to an incoming UAS.

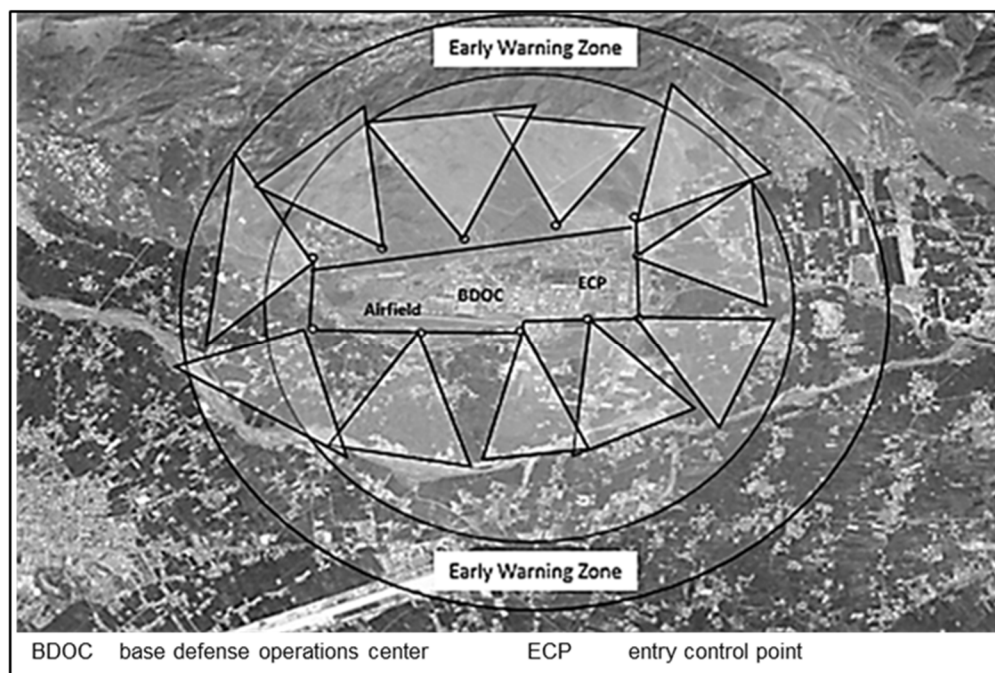


Figure 4-5. Observation points

REACT TO THREAT UAS

4-46. Understanding the capabilities and limitations of UAS can increase a Soldier's ability to react and defeat a threat. Reacting to a threat UAS should include reporting to the operations center and security personnel if the UAS does not pose an immediate threat. Defeat does not equate lethal means; however, it is an option. Other defeat solutions could be limiting a surveillance threat from gaining information or following the air path of the UAS to the operator.

4-47. Techniques for reacting to UAS include:

- Treat unidentified UAS as enemy and/or with hostile intent.
- Use visual, electromagnetic, or procedural means to detect, track, and identify threat UAS.
- Initial spot reports must be sent to higher headquarters to facilitate the identification process.
- Once a UAS is identified, simultaneous processes begin thereafter.
- Commanders have discretion to initiate a quick reaction force and begin the target defeat decision.
- All target defeat decisions must be given by an engagement authority and receive airspace deconfliction/clearance.
- Dependent on the mission and the best method of engagement, lethal or non-lethal engagement responses come from fixed-site or mobile systems.
- After engagements have ceased, the battlespace owner conducts a cordon and search to locate the down UAS. The battlespace owner then submits a 9-line report to request explosive ordnance disposal (EOD), and support to render safe the downed UAS.

- Once EOD renders safe any explosive hazards, weapons intelligence or other analysis can commence on the downed UAS.
- All reports must be sent within the respective theater's reporting timeframe of engagement to higher headquarters.

4-48. Figure 4-6 is a simplified flow chart showing the process from UAS detection to submission of the final report to higher. Leaders must be aware that local standard operating procedures may dictate other steps and requirements.

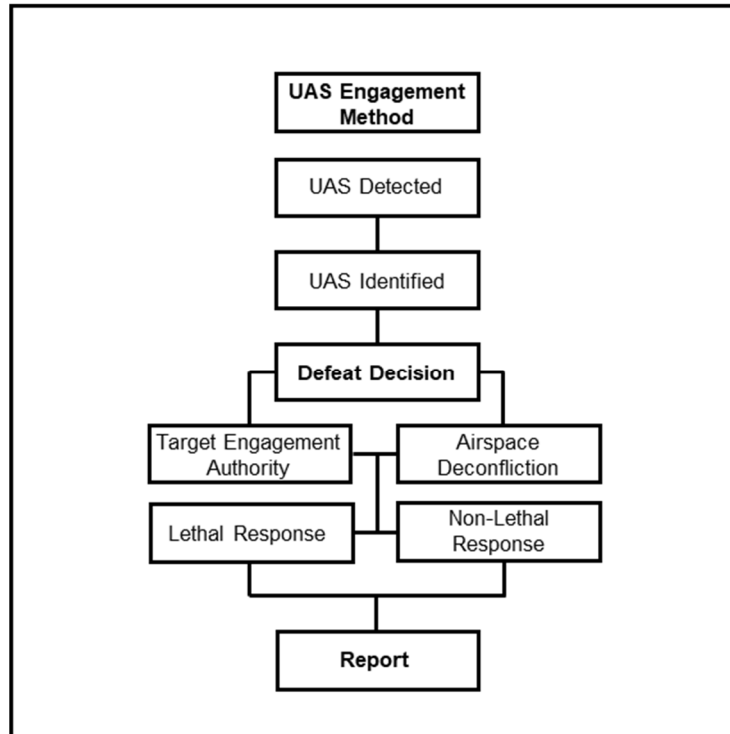


Figure 4-6. Unmanned aircraft system reporting flow chart

DETECT

4-49. Detection is priority in counter-UAS operations. Smaller platforms are used for supportive functions such as detection, targeting assistance, or surveillance prior to an actual attack. There are three methods of identification: visual, procedural, and electromagnetic.

4-50. Visual Aircraft Recognition (VACR) is an established method of visually identifying the type of aircraft in flight. Visual aircraft recognition can distinguish the UAS physical form based on its configuration. Multiple configurations exist; a few examples are rotary-wing, fixed-wing, hybrid, tiltrotor, or a combination of all.

4-51. Procedural detection depends on UAS behavior in flight. Airspace coordinating measures that are not followed, point of origin, erratic behavior, and loitering above important locations are all behaviors that illustrate non-friendly or hostile behavior. Rotary-wing platforms can hover and collect intelligence, while Fixed-wing platforms can make several passes to achieve the same fidelity as a rotary-wing. These behaviors are indicative of intelligence-gathering platforms and can be likely be categorized as meeting hostile intent of intelligence platforms and can be detected as unordinary with hostile intent.

4-52. Electromagnetic detection is generally the fastest detection method. It requires special equipment to detect the operational controls of the UAS. Sensors can identify targets based upon radar cross-section, infrared signatures, and other electromagnetic signatures that UAS exhibit within the EMS. See figure 4-7, C-UAS Time/Distance Engagement Sequence Planning Considerations, for a linear depiction of this process.

TRACK AND IDENTIFY

4-53. Tracking UAS is possible with several systems and personnel. System integration with multiple sensors is the best method to maintaining situational awareness of UAS. Tracking is achieved by multiple means of active and passive sensing measures and integrating them with current C2 infrastructure and systems. Some passive sensor systems receive RF downlink cues from the UAS while active sensor systems will use radar to track the UAS. Planning considerations for tracking include line-of-sight limitations, terrain obstruction, urban environment obstructions, and the operational RF environment. Many frequencies are shared with UAS and must be identified before classifying as hostile or using mitigation techniques. See figure 4-7 on page 38, C-UAS Time/Distance Engagement Sequence Planning Considerations, for a linear depiction of this process.

4-54. After initial detection, tracking and identification will follow. There are multiple ways to identify UAS. A common method is the "wings, engine, fuselage, tail" (WEFT) identification method. The presence of wings or rotors determine the type of UAS. Most UAS are propeller driven, from either a single propeller for propulsion with wings or multiple props mounted on top of arms to provide hover capability. The fuselage will maintain and house internal components. In addition, the presence of a tail for assisting in maneuvering can identify the type of UAS. Through joint processes and procedures, identification is achieved. As mentioned before, UAS that do not adhere to airspace control measures can then be deconflicted and identified as a friendly with an emergency, an unknown with hostile intent, or hostile aircraft.

DEFEAT

4-55. Defeat techniques begin once airspace deconfliction and target engagement authority has been passed down to the tactical level. To confirm the identity of the UAS and prevent fratricide, multiple processes and procedures must be initiated. Depending on the engagement method, area RF deconfliction may be required. Depending on the frequencies, there may be opportunities where operational RF spectrums overlap with the control frequency of the UAS. Key leaders must determine and mitigate frequency fratricide during defeat measures. Defeat measures can follow non-lethal or lethal procedures. During non-lethal responses, it is crucial to continue jamming until the craft is inoperable. After lethal or non-lethal responses, and once the UAS has shown no control-link, EOD must render the UAS safe. Once the UAS is rendered safe, the craft may be exploited for weapons intelligence or other analysis.

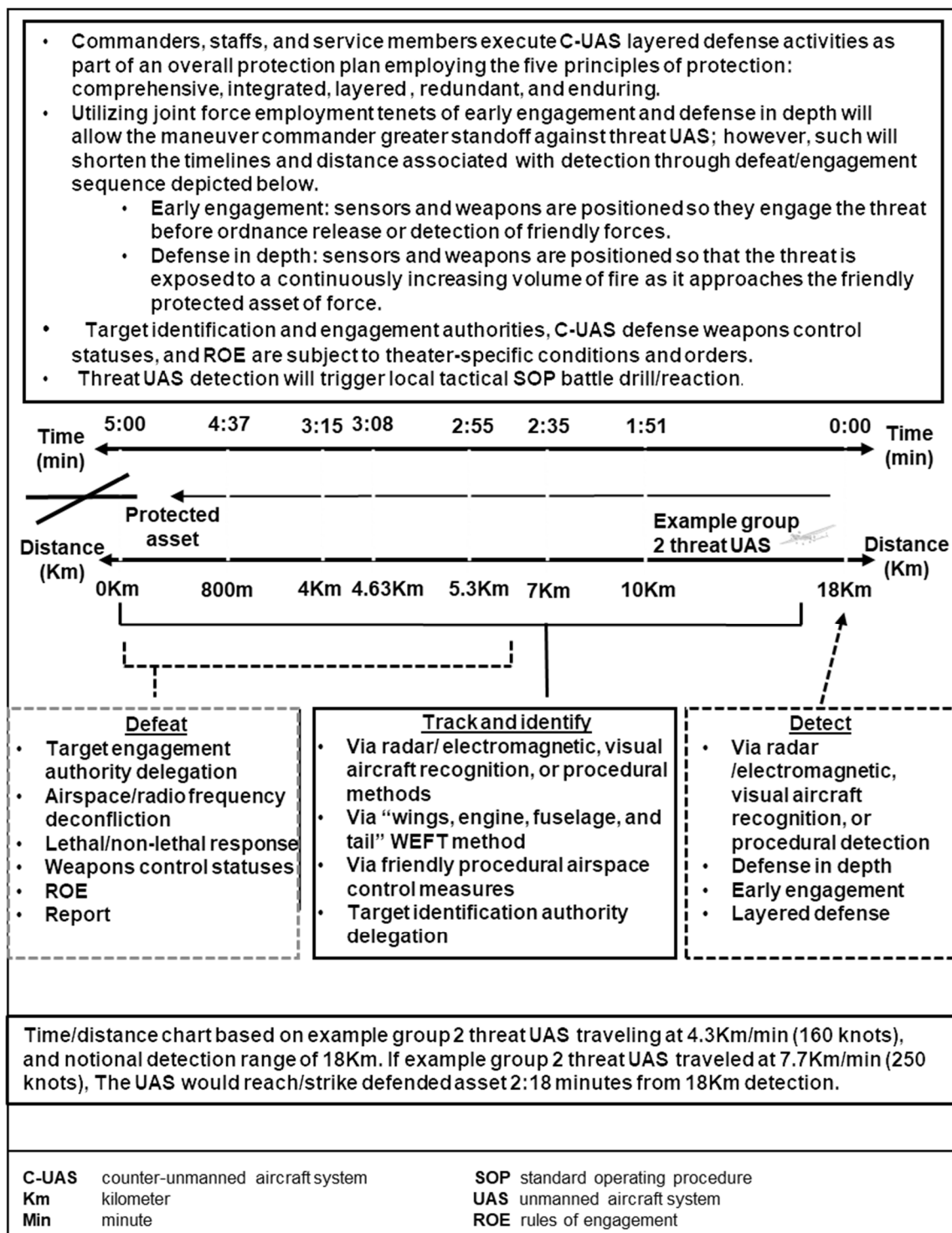


Figure 4-7. Counter-Unmanned Aircraft System time/distance engagement sequence planning considerations

REPORTING REQUIREMENTS

4-56. Reporting requirement timeframes are based on which unit level is submitting the report. It is expected that company, battery, troop level spot reports and engagement reports are sent up according to their theater

specific timelines. The initial spot report drives the UAS battle drill. Without the important information captured, the chain of command cannot make essential decisions based on UAS payload, intent, type, and possible endurance. Fixed-wing UAS have more endurance than rotary-wing aircraft. This essential piece of information can help decide what types of missions the platform can conduct. If the type of UAS payload can be identified, there may be ample time to warn friendly personnel about possible fragmentary, anti-personnel, or surveillance payloads that may affect operations.

DOWNED UAS

4-57. Soldiers may encounter a downed UAS. When this occurs, Soldiers will treat the UAS as an improvised explosive device with active ISR capabilities. The best practice for these situations is to conduct the five "C's" (confirm, check, clear, cordon, control) while maintaining visual contact from a safe distance of the downed UAS:

- Confirm-Use optics for stand-off, look for indicators/presence of suspicious items (does it look modified, is there a payload?).
- Check-Conduct 5/25/200-meter check for dropped payload or additional grounded UAS.
- Clear-Clear non-essential personnel from the immediate area.
- Cordon-Cordon off the area to preserve the scene for exploitation and provide protection/security from command/victim-initiated improvised explosive device.
- Control-Allow only authorized access to the site, maintain visual LOS to the UAS.
- Report status to the operations center.

This page intentionally left blank.

Chapter 5

Passive and Active Defense

This chapter discusses both passive and active defense with respect to the air environment. Passive air defense are measures that units may employ to safeguard its personnel and equipment from air threats. Units may be in a situation where they are vulnerable to attack or taking unnecessary casualties. In cases where the enemy aerial platforms are outside the range of the unit's weapons, a unit's most lucrative option can be to disperse and seek cover. Commanders must prepare their units to actively engage air threats if attacked. The decision to engage air threats should include consideration of the unit's mission and tactical situation.

PASSIVE DEFENSE

5-1. Combined arms forces and small units should be ready to employ passive defense measures to protect themselves from detection, observation, and attack. Passive air defense is all measures, other than active defense, taken to minimize the effectiveness of hostile air and missile threats against friendly forces and assets (JP 3-01). Passive defense measures decrease the effectiveness of enemy attacks using UAS against friendly forces and their assets. Units must train their forces to avoid direct and indirect attacks from air threats. Two types of passive measures are damage-limiting and attack avoidance measures.

5-2. Commanders employ passive air defense measures to improve their units' survivability by increasing the likelihood of not being detected and targeted (attack avoidance) from the air and by mitigating the potential effects (damage-limiting) of an air attack (ATP 3-01.8). ADA units provide threat identification and site alarming by disseminating early warning. Units will not always have a dedicated ADA element available to prevent air attacks. Conducting passive air defense measures routinely may decrease the chance of detection or limit the damage from an air attack.

5-3. The air defense coordination/management officer in the brigade combat team ADAM/BAE is responsible for ensuring that all brigade combat team elements (staff, organic units, and attached units and personnel) understand and employ the necessary passive defense measures to mitigate the effectiveness of enemy UAS. Passive air defense measures are the first line of defense against UAS. Based on the unit's assigned mission and ROE, the commander will have to decide whether to engage any approaching hostile aerial platform.

PASSIVE DEFENSE TASKS

5-4. When planning damage-limiting and attack avoidance measures units should consider, and subsequently train their forces, on the following passive defense tasks:

- Operate at night or during limited visibility. Affects threat UAS observation but also limits the unit's operational support. Organizations must assume that the enemy has the capabilities to conduct limited visibility or night operations. Units at all levels need to ensure proper training is conducted during hours of limited visibility. Practice light restrictions and discipline.
- Establish an early warning network. Establish an air defense early warning network using the radios and digital networks that are assigned to the unit command post. Ensure that supported units have trained and assigned personnel to always monitor these networks and radios.
- Disseminate early warning of air threats to the lowest echelon. Early warning from the highest to the lowest echelons is essential to countering the UAS threat. Upon detection and classification of enemy UAS, the brigade must relay alert information on locations, altitudes, and time to surrounding ground forces. This information will be vital to the ground forces protection and the possible capture of the UAS and its ground platform. Automated early warning of UAS is disseminated throughout the brigade's common user network down to the lowest echelons.
- Practice good operational security. Operational security is an essential part of the unit's planning process. Commanders and leaders must always enforce their units' operational security measures. A unit must implement countermeasures immediately upon detection of an enemy UAS. Practicing good operational security will safeguard critical information and reduce the unit's vulnerabilities to

enemy collection efforts. Developing and employing basic countermeasures and TTP, such as limiting the number of times friendly forces are exposed to possible aerial observation or minimizing organized unit activities until the threat is neutralized or destroyed, should be considered.

- Use emission control to limit electromagnetic and acoustic footprints. The controlled use will also mitigate detection by enemy sensors, mutual interference among friendly systems, and enemy interference with the ability to execute a military deception plan.
- Unit dispersion. Disperse assets to minimize detection and damage if attacked. Dispersion may be the best damage-limiting measure. Proper dispersion of a unit and equipment lessens target density and reduces the lethal effects of the ordnance used against that organization. Area weapons become less effective when units disperse.
- Maintain vigilance. Friendly forces must assume they are always vulnerable to enemy targeting attempts. This is especially true when conducting convoys for troop movements or performing supply actions and as they move through open areas or concentrate at choke points along the convoy route.
- Survivability techniques. These are specific groups of tasks that enhance survivability. When existing terrain features offer insufficient cover and concealment, altering the physical environment to provide or improve cover and concealment enhances survivability (engineers are typically required for these tasks). Similarly, using natural or artificial materials such as camouflage may confuse or mislead the enemy or adversary. Together, these are called survivability operations—those protection activities that alter the physical environment by providing or improving camouflage, cover, and concealment. See figure 5-1 for examples of survivability techniques. Survivability focuses on using:
 - **Camouflage.** This is the use of natural or artificial materials on personnel, objects, and tactical positions to confuse, mislead, or evade the enemy.
 - **Concealment.** This makes use of terrain and other natural or man-made features to protect from observation and surveillance. Concealment is used to reduce the factors of recognition.
 - **Hiding.** Hiding is the concealment of an object by some form of natural or man-made screening. Hiding screens is a method to screen a target from enemy sensors. This can include the use of obscurants such as optical and noise reducing measures to limit the glare or noise of equipment. Place mud on headlights and use camouflage nets to obscure the glare of windshields. Use noise blocking barriers and foam to lower the noise of operating equipment.
 - **Blending.** Blending is the arrangement or application of camouflage materials on, over, and around the object so that it appears to be part of the background.
 - **Disguising.** This is the application of materials on a target to mislead the enemy as to its identity. Clever disguises can often mislead the enemy concerning identity, strength, and intention, and may draw fire away from real assets.
 - **Disrupting.** This includes actions or techniques that alter or eliminate regular patterns and target characteristics.
 - **Decoys and deception.** Using such things as decoys to set up false locations, with smoke to draw attention away from an operation, or emitters and emulators to confuse collection activities can conceal unit activities from enemy detection.
 - **Cover.** Cover and hardening use protective construction and overhead cover to provide damage-limiting cover for friendly forces and equipment. The hardening and fortifying of cover will limit the threat UAS ability to visually see and limit the damaging effects of an aerial attack. Hardened overhead cover mitigates the effects of improvised munitions delivered by threat UAS on assets such as fighting positions; operation centers; petroleum, oil, and lubricant sites; ammunition supply points; critical communication nodes; and other assets deemed critical by the commander.
 - **Compartmentalization.** Compartmentalization refers to dividing a large, facility, area, or individual assets into smaller components. This can be accomplished within a smaller footprint through use of ballistic-resistant walls. It can also refer to separation of components/elements across a wider area to reduce risk from blast/impact.

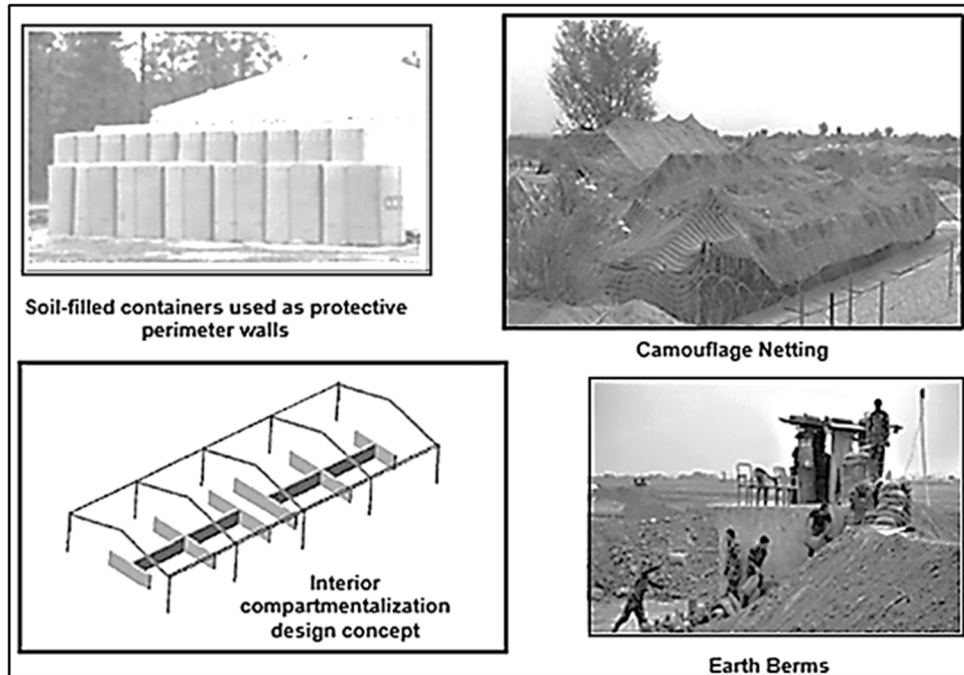


Figure 5-1. Examples of survivability techniques

VISUAL AIRCRAFT RECOGNITION

5-5. A unit's area of operation can be the deciding factor for types of UAS that will be seen in the area. Increased UAS capabilities have increased the demand for visual aircraft recognition and understanding is critical at the Soldier level. Due to their small radar cross section and low/slow/kinematic profile, it is difficult to detect and identify using radar systems. VACR helps distinguish between UAS primary physical forms (rotary-wing, fixed-wing or hybrid) to assist in combat identification. The traditional method of aircraft identification is wings/engine/fuselage/tail. Wings/engine/fuselage/tail is the accepted system of aircraft identification based on the aircraft's individual features. Wings/engine/fuselage/tail is a memory aid used in training VACR. UAS must be detected, recognized and then identified at the farthest range possible. Early detection aids leaders with making timely decisions to report and possibly engage UAS. The farther out an aircraft is positively identified, the more time is given to make engagement decisions. Estimation of search limits/visual technique (see figure 5-4 on page 49), vertical scan and search (see figure 5-5 on page 49), horizontal search and scan (figure 5-6 on page 50) are a few techniques that can be utilized to detect and identify UAS.

AIR GUARD

5-6. Assigned Soldiers need to be vigilant with eyes on the horizon. They will perform actions such as search and scan techniques for approaching threat UAS while observing their assigned sectors (see figures 5-4 on page 49 and figure 5-5 on page 50 for air guard scan techniques). Early warning is key to alerting formations of any possible air threats. Sectors must cover likely avenues of approach for threat UAS. Soldiers can potentially engage threat UAS if they are equipped with dismounted C-UAS assets in accordance with ROE and weapon control status.

5-7. Reporting threat UAS activity should include an estimate of the threat(s). This information should include reference points based on known locations, such as the air guard's position, a friendly unit's grid coordinates, or major terrain feature. Using this method can assist others in accurate locating and targeting the threat UAS. The air guard reports the approximate distance, time, duration, size, estimated elevation, and direction the UAS was heading when detected. If a low flying UAS is spotted, the air guard should immediately be on alert to identify any possible threats in close proximity, to include enemy ground troops or control teams. When spotting a UAS, compromise of the air guard's position is possible.

5-8. Reporting of a threat UAS should utilize a standard reporting format. This ensures all Soldiers understand the process and information required to conduct an enemy spot report. Routine reporting allows units time to quickly adjust force protection measures and coordinate immediate response to UAS threats. Unit C-UAS TTPs must be tailored to the expected threat environment in one's AO. That means creating a TTP that focuses on setting priorities on specific lines on a spot report above other. Units can also tailor their reports to address the UAS situation by adding the reported UAS's approximate speed, heading, and altitude in line 4. When reporting UAS activities the reporting element may also add UA platform characteristics into line 3 instead of just the reported platform's size alone. Those characteristics may include if the UA is a quadcopter, fixed-wing, or single rotary platform. See table 5-1 on page 46, for an example of a spot report format for threat reporting. Table 5-2 on page 47, provides an example of the 16-line report that must be completed within 24 hours. Table 5-3 on page 48, provides an example of the engagement report that must be completed within 48 hours of a UAS engagement.

AIR GUARD POSITIONING

5-9. Air guards can be the first line of defense when detecting and coordinating enemy UAS location and direction. The commander of each unit typically selects them, but selection can be delegated down to other leaders. Air guards are responsible for spotting aerial threats within close proximity to the unit's location. They search for aerial targets using search and scan techniques.

5-10. Position air guards in in-depth (see figure 5-2) or linear positions (see figure 5-3). Air guards placed in-depth can be configured as completely vehicle-mounted air guards, dismounted air guards forward of the vehicle, or a combination of the two. In-depth air guard placement allows the company to observe its entire sector. This method works well when the company has assigned platoons sectors that contain terrain that facilitates multiple UAS avenues of approach, is heavily vegetated, or contains civilian infrastructure that provides the enemy with cover and concealment. In-depth placement allows for redundancy in observation and better interlocking coverage of the sector. Linear placement is effective when the enemy is not moving and provides optimum observation of the enemy.

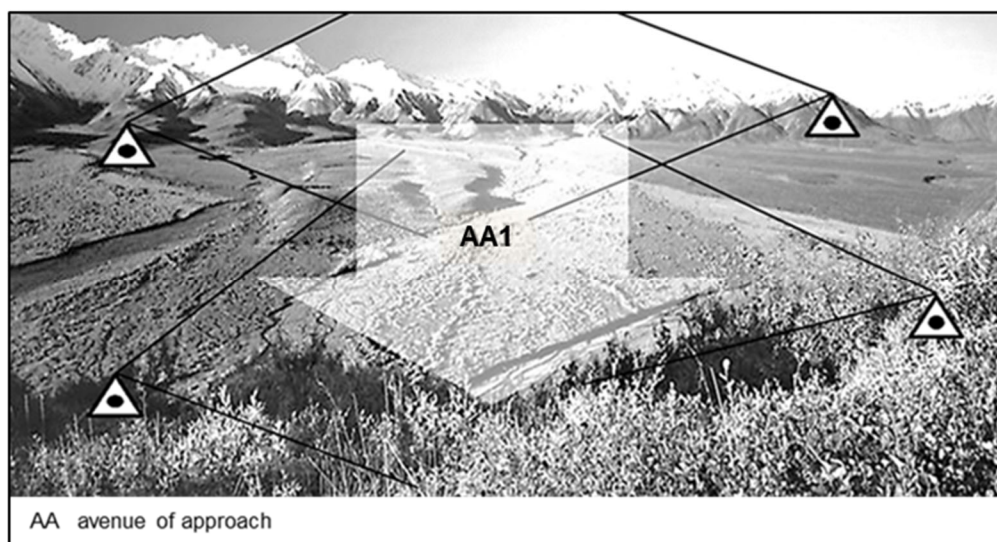


Figure 5-2. Positioning in-depth



Figure 5-3. Positioning linear

5-11. Based on mission tasks, air guards use the standard quick reference or pre-deployment and combat checklists developed by the brigade to focus on C-UAS tasks. The checklist should be available through standard military digital devices or in hardcopy form and include-

- Current UAS trends (type classification).
- Types and characteristics of UAS.
- Specific data on local air threats and named areas of interest.
- C-UAS equipment available.
- Secure radio operations and frequencies.
- Unit call signs to request support (quick reaction force or ADA element).
- Military map of the area.
- Binoculars and night vision devices.
- Orientation techniques (location, heading, speed, and line-of-sight).
- C-UAS spot report (see table 5-1 on page 46).

Table 5-1. Example Counter-Unmanned Aircraft System Detection Report (SALUTE Format)

<i>Line</i>	<i>Information</i>	<i>Example</i>
1	Size	Report the number of unmanned aircraft systems (UAS), or size of the formation.
2	Activity	Report detailed account of actions: What is the UAS's direction of movement? Was there any hostile action? Is the threat UAS loitering in one spot? Is it flying straight? Was the threat UAS approach observed or was it spotted overhead?
3	Location	Report where you saw the activity. Include 6 to 8- digit grid coordinate of reporting element and either grid or distance and direction from reporting element location (known point).
4	Unit (Description of UAS)	Include details such as: • Fixed-wing or rotor/multi-rotor. • If fixed wing. • Estimated length of wingspan. • Tail configuration. • If rotor/multi-rotor. • Number of rotors. • Height. • Payload, sensors, and weapons. • Any lights. • Other distinguishable markings.
5	Time	Report the time the activity was observed.
6	Equipment	If possible, report all equipment associated with the UAS, such as payload or weapons.

Table 5-2. 16-Line Report (Incident)

Line	Information	Example
1	Base or Facility name	Report the State / Country
2	Date Time Group (DTG) of the incident or incursion (Zulu) and duration.	Report using DDHHHH Zulu MMMYYYY format.
3	Geographic area	Report either USAFRICOM, USCENTCOM, USEUCOM, USINDOPACOM, USNORTHCOM, or USSOUTHCOM
3a	Reporting service / Component	Report either Army, Navy, Air Force, Marine Corps, Space Force, Coast Guard, National Guard, Air National Guard, or other.
4	Unit / Organization Contact Information	Report the Unit / Organization, Name, Rank/Grade, E-mail, and Phone Number.
5a	Geo-location of the incident or incursion	Report the Latitude-Longitude or MGRS of the observer / sensor to the UAS
5b	Location name	Report utilizing standardized naming convention.
6	Incident or incursion environment	Report either United States, Host nation, Theater of War, or International Waters.
7	Total number of UAS detected	Report the number of UAS detected in the format of (1-XXX)
8	First Detection	Report Outside installation / outside Installation-restricted area / within installation-restricted area / mobile
9	Detection method	Report if detected utilizing visual, radar, electronic, EO-IR, acoustic, or other means.
10	UAS airframe	Report the type of UAS either fixed wing, rotary wing, unknown, and other
11	UAS detailed description	Report the number of rotors, number of lights, light pattern (blinking or solid), color of lights, payload, movement pattern, and other features.
12	C-UAS equipment Operational	Report yes, no, unknown, or N/A
13	UAS engaged	Report Yes (engagement report, CJCS and CCCR CCIR), No, or N/A
14	UAS incident or incursion has a mission impact (commanders' assessment)	Report Yes (CJCS and CCCR CCIR) or No.
15	UAS incident or incursion unsafe / unprofessional (commander's assessment)	Report Yes (CJCS and CCCR CCIR) or No.
16	UAS incident or incursion narrative	Create a detailed narrative describing the UAS incident or incursion.
Legend		
DTG date time group		MGRS military grid reference system
UAS unmanned aircraft system		EO electro-optical
IR infra-red		

Table 5-3. Example Unmanned Aircraft System Engagement Report

Line	Information	Example
1	Title	Report Base or Facility name; State/country
2	Engagement start Date TIME Group (DTG) (Zulu)	Report using DDHHHH Zulu MMMYYYY format.
3	Total time of initial / follow-on engagements	Report using the HHMM format
4	Type of engagement	Report RF / Kinetic / C-PNT / other
5	C-UAS engagement Effective?	Report Yes / No / Unknown
6	Any confirmed electronic / collateral effects from C-UAS systems	Report Yes / No / Unknown (explain in narrative, line 11)
7	Was the UAS confiscated and / or captured?	Report Yes / No / Unknown
8	Attribution: Was the UAS operator located and / or interviewed?	Report Yes / No / Unknown / N/A (explain in narrative, line 11)
9	FAA and / or Host nation equivalent notified:	Report Yes / No
10	Is video and / or photo available?	Report Yes / No / N/A
11	UAS engagement narrative	Report if confiscated and / or captured explain who has it
Legend		
DTG date time group		C-UAS counter unmanned aircraft system
FAA Federal Aviation Administration		

5-12. Soldiers should have the ability to conduct all operations under all conditions: day, night, and limited visibility. They should be equipped with the necessary optical gear to perform search and scan techniques to reduce the enemy's ability to evade detection. The following figures illustrate search limits, search, and scan methods. Refer to TC 3-01.80 for details on search and scanning techniques.

5-13. When searching and scanning for UAS, do not limit the search too near the horizon and miss higher-flying aircraft or search too high above the horizon and miss lower flying targets. The correct upper limit of search is 20 degrees above the apparent horizon (see figure 5-4).

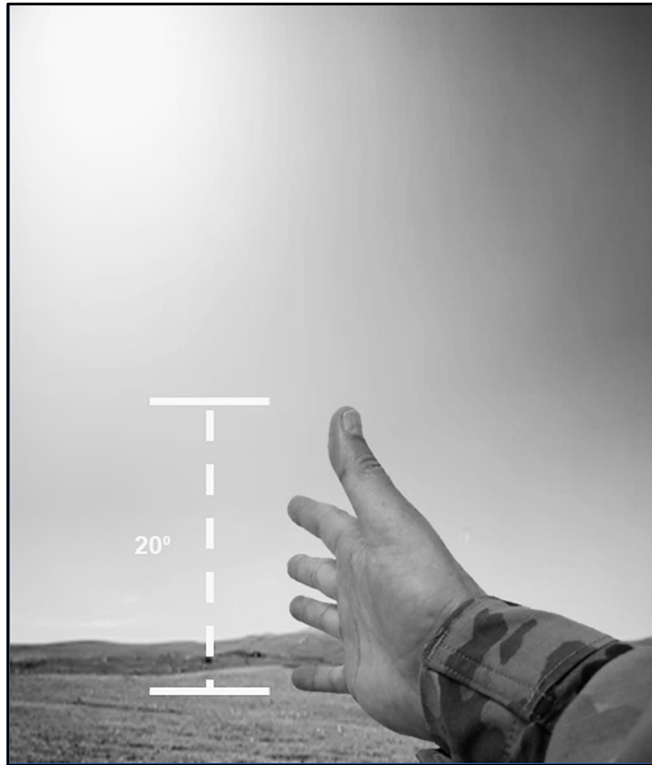


Figure 5-4. Method of estimating 20 degrees

5-14. The vertical scan is the technique used to optimize vision for finding air threats (see figure 5-5). By using quick eye movements upward toward the sky, then downward to the horizon and continuing across the terrain, the air guard should scan using the same pattern to approximately 20 degrees below the horizon to compensate for all UAS.

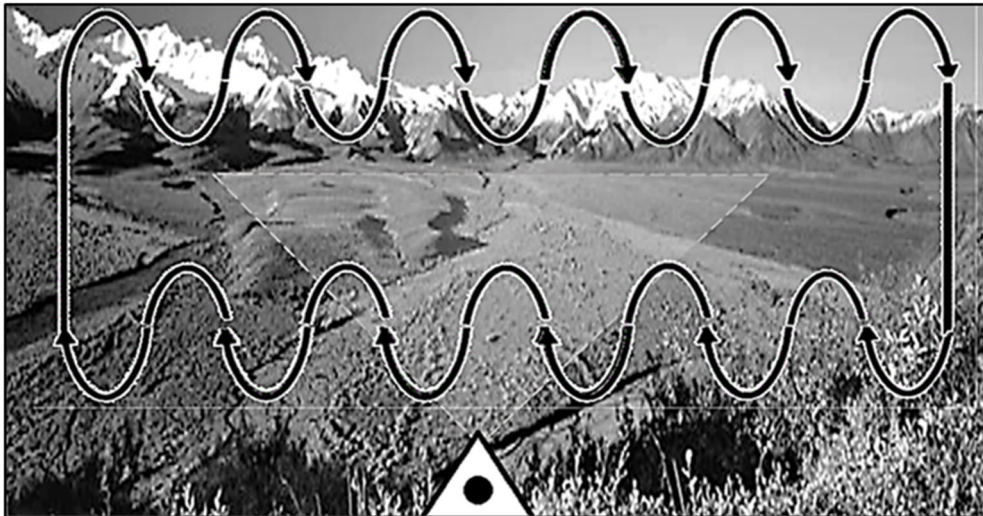


Figure 5-5. Vertical scan technique

5-15. In horizontal scan viewed from the horizon (see figure 5-6 on page 50), the air guard should search using short, quick eye movements across the sky while working upward to approximately 20 degrees. As in vertical scanning, the air guard should continue the search and scan technique to 20 degrees below the horizon to detect aircraft flying nap of earth.

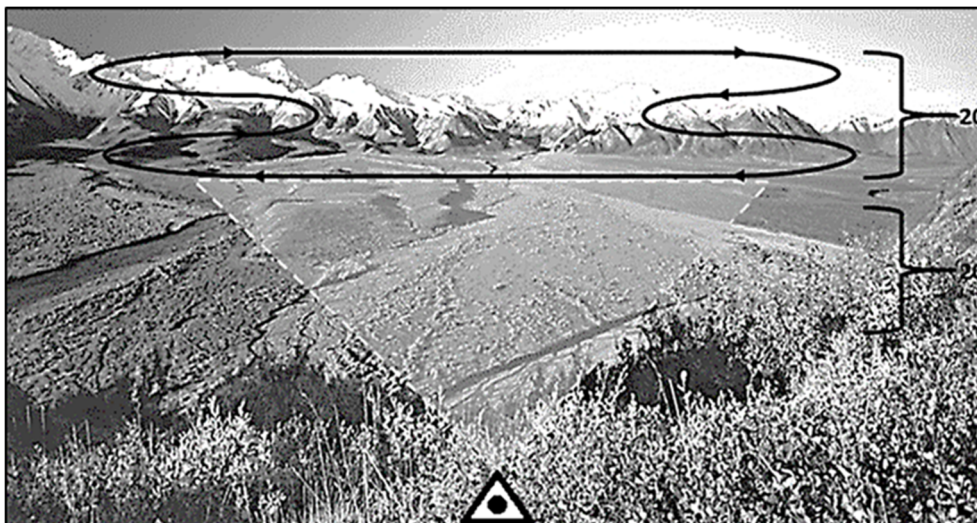


Figure 5-6. Horizontal scan technique

5-16. Understanding how to apply C-UAS observation techniques enhances reaction and reporting time, thus increasing survivability. Air guard proficient in applying terrain analysis and map reading techniques may be able to determine probable enemy launch locations using the UAS's direction of approach.

5-17. Commanders and leaders must conduct rehearsals to train and educate air guard personnel on their specific responsibilities and standard operating procedures for reporting the UAS threat. Rehearsals will provide company commanders the ability to make any needed changes and verify the proficiency of personnel to conduct air guard techniques.

AIR GUARD CHECKLIST

5-18. The company commander should consider planning for redundancy in positioning guards. The need for redundancy may be dictated by the terrain, threat assessment, or overall importance of the mission. Air guard redundancy ensures sustained observation, enabling the unit to continue the mission if the enemy compromises some air guard positions.

5-19. Before assuming duty as an air guard, leaders perform precombat inspection to ensure the designated air guard has the correct equipment and has been briefed on the current threat. The air guard checklist includes, but is not limited to:

- Understanding on types and characteristics of threat UAS.
- Understanding of current UAS trends.
- Specific data on local air threats and named areas of interest.
- Detection equipment (such as binoculars, night vision devices, and thermal weapon sights).
- C-UAS equipment available.
- Secure radio operations and frequencies to send out early warning.
- Unit call signs to request support.
- Military map of area.
- Orientation techniques (location, heading, speed, and line-of-sight).
- C-UAS Range card.

ACTIVE DEFENSE PLANNING

5-20. Active air defense is a direct defensive action taken to destroy, nullify, or reduce the effectiveness of hostile air and missile threats against friendly forces and assets. It includes the use of aircraft, air defense weapons, electromagnetic warfare, and other available weapons (JP 3-01). Active defense of UAS requires early detection to permit acquisition, tracking, classification, identification, and destruction as soon as possible.

5-21. Active air defense plans must be coordinated with airspace managers and ADA personnel. These plans should consider the use of air defense weapons, small arms, EW, and any other assets available to the brigade that can detect and mitigate hostile aerial platforms.

5-22. Active air defense planning measures taken in support of the mission must adhere to the ROE and weapons control status and consider potential collateral damage associated with the weapon system to the surrounding area.

ACTIVE MEASURES FOR C-UAS

5-23. **Active defense** measures are a multi-step sequence that units and service members do to detect, track, identify, decide, and potentially engage an unknown UAS. The quicker these steps can be applied, the more effective the response against threat UAS (JP 3-01).

Detect

5-24. UAS are small, maneuverable, and quiet. Even to the trained eye they are often very difficult to observe in flight. Environmental conditions can make such systems difficult to detect without the use of special technological tracking and identification devices. Time of day, ambient light levels, meteorological conditions, and observer alertness will all impact on the ability to observe a potential hostile UAS. Moreover, an experienced operator can fly a UAS in a tactical manner as such to further enhance the ability to exploit UAS characteristics. This may include:

- Flying at low level, using terrain, obstacles with vertical extent and/or urban environment to mask an approach to a potential target location.
- Making a series of false take-offs and approaches to intended target location.
- Use of erratic, dynamic flight profiles to confuse and deceive personnel, making visual observation challenging.
- Using the sun or cloud cover to effectively mask the UAS from sight.
- Flying upwind approaches to minimize the ability to detect the sound of the UAS.
- Use of sport flying modes to increase speed and agility and minimize the time to observe the UAS.
- Use of multiple UAS to confuse, deceive, and overwhelm observers and make tracking leading to defeat more difficult.
- Flying a pre-programmed flight profile to minimize risk to the operator, allowing for the link to be disconnected in flight from the control station and re-established over the target area from another position.

5-25. The types of sensors and their placement determine the unit's detection capability. Threat UAS types, threat axis of advance, terrain, weather, time-distance analysis, friendly defended assets, desired engagement zone, surveillance requirements, and the number of available assets impact how best to place and employ sensors. For sensor placement, integrating and networking sensors to develop the enemy threat UAS situation should be applied. The use of various types of sensors is warranted as currently there is no one type of sensor that is 100% effective.

5-26. Various sensor capabilities outside of visual (observer) could include radar, radio frequency, audible, and optical devices. The goal is to form an integrated sensor network that includes various sensor types. Sensor capabilities in support of low-level air threats are planned accordingly and coordinated in advance. Leaders may have to coordinate through higher echelons for additional sensor capabilities. No matter what sensor capabilities a unit has, all service members need to be aware of the air threats and constantly look up before and during any movements. Dedicated air guards are another way units can assist in air threat detection and engagement.

TRACK

5-27. Simultaneous with providing warning, friendly forces track the UAS and monitor its movement. Keeping track of the UAS needs to occur until a decision is made to engage or not engage the UAS and is successful. A location is a static estimated report or display of where an air threat is located at a given moment. A system track is a compilation of location reports over a set period. Depending on the system employed the system track can be reported as a heat map display, quadrant alert, or a circle to indicate

estimated center and location error or line of bearing. The detection plan contributes directly to the unit's ability to track airborne objects continuously and efficiently.

IDENTIFY

5-28. Identification is the process of determining the friendly or hostile characteristics of an unknown detected contact. The employment of C-UAS capabilities requires early identification of UAS to maximize engagement times and avoid fratricide. The problem of distinguishing friendly, neutral, and hostile aerial objects while employing various weapon systems against threat UAS is a highly complex task. Service members need to be familiar with the characteristics of friendly UAS operators in the area. The same UAS may be flown by both friendly and enemy forces. Accurate identification allows leaders to make engagement decisions and enhances situational awareness. Timely identification improves weapons employment options, helps conserve friendly resources, and reduces the risk of friendly fire.

5-29. There are two methods of identification, procedural and positive. Positive identification is the preferred method of operation, but generally, some combination of positive and procedural identification is used. Procedural identification separates airspace users by geography, altitude, heading, time, and maneuver. Positive identification is derived from observation and analysis of UAS characteristics including visual recognition, electronic support systems, non-cooperative UAS recognition techniques, identification friend or foe systems, or other physics-based identification techniques in accordance with JP 3-01.

5-30. Identification of a UAS should lead to a specific name or category or the exact make and model of the UAS. Identification of its payload is also important if it can be determined. The process of assigning an identification to a track likely will depend on several criteria. Characteristics that assist in identifying an unknown UAS include identifying:

- If fixed wing-
 - Estimated length of wingspan.
 - Tail configuration.
- If rotor/multi-rotor-
 - Number of rotors.
 - Height

DECIDE

5-31. Decide consists of two decisions. First, whether there is a need to engage. Second if the decision to engage is made, the methods used to lessen or eliminate the threat posed by a UAS. These methods include physical and nonphysical. Some organizations will be equipped with cyber capabilities which include both physical and nonphysical methods. The degree of delegation is consistent with the ROE, the available airspace, potential for collateral damage, and the inherent right of self-defense.

5-32. Physical methods engage with and either destroy or damage the device so that it is not operational. Examples of physical methods include, but are not limited to:

- Explosive munitions
- Small arms
- Projectiles
- Entanglement
 - Streamers
 - Spray foam
 - Capture nets
- Directed Energy
 - Laser
 - High-power microwaves

DEFEAT

5-33. Defeat techniques begin once airspace deconfliction and UAS engagement authority has been passed down to the tactical level. To confirm the identity of the UAS and prevent fratricide multiple processes and procedures. Depending on the engagement method, area radio frequency (RF) deconfliction may be required. Depending on the frequencies there may be opportunities where operational RF spectrums overlap with the

control frequency of the UAS. Key leaders must determine and mitigate frequency fratricide during defeat measures. Defeat measures can follow non-lethal or lethal procedures.

5-34. During non-lethal responses, it is crucial to continue jamming, until the UAS is inoperable. After lethal or non-lethal responses, and once the UAS has shown no control-link, explosive ordnance disposal (EOD) must be requested to render the UAS safe. Once the UAS is safe, the UAS may be submitted for weapons intelligence and analysis.

ENGAGE

5-35. Commanders have the responsibility to take whatever action is necessary to protect their forces and equipment against attack and ensure their Soldiers operate in accordance with established ROE. The air defense ROE must be adhered to when conducting engagements against UAS. Commanders at all echelons must exercise the right of self-defense to protect their forces from UAS. Hostile criteria for identification of UAS must be delegated as low as possible to facilitate C-UAS operations. Weapons control status for engagements against UAS must be as permissive as possible. The air defense staff at the brigade, division, and corps must ensure that conditions are set for a permissive fight at subordinate echelons against enemy UAS.

5-36. Once a decision is made to engage a threat UAS the capability will then be decided, the determined capability engages the threat UAS neutralizing the target or destroying it. Other C-UAS capabilities will continue to track the threat UAS in case the target was initially missed, and they can engage or re-engage as necessary.

Small Arms Techniques for Engaging UAS

5-37. Small arms techniques used in air defense incorporate the use of volume fire and proper aiming points according to the UAS direction. If service members are trained to apply an appropriate sequence of engagement techniques for UAS based on the rules for selecting aiming points, the response will be automatic upon command. Small arms are limited to the range and destructive capability of the weapon and should be used only on low flying UAS.

5-38. The decision to fire small arms against threat UAS is the unit commander's and is based on the situation. Considerations should at a minimum include the severity of the threat versus the potential impact of the unit's effectiveness and the area of engagement (urban versus rural).

5-39. Soldiers that encounter UAS should consider them as a threat eligible for engagement unless positively identified as friendly. UAS can fly extremely low underneath traditional radar detection zones. They can fly very slowly with the ability to hover in place, preventing sensors from detecting them. They can also fly quickly, making it difficult to track them.

Volume Fire

5-40. Volume fire is an effective method to employ when using small arms fire against aerial threats. The key to success in engaging enemy aircraft with small arms is to put out a high volume of fire towards the immediate threat. The more bullets a unit can put in the sky, the greater the chance the enemy will fly into them. Even if these fires do not hit the enemy, throwing up a "wall of lead" in the sky can intimidate threat UAS pilots, ultimately breaking off their attack or distracting them from taking proper aim. One of the most important points about volume fire is that once the lead distance is estimated, you must aim at the estimated aiming point and fire at that single point until the aircraft has flown past that point. Maintain the aiming point, not the lead distance. Once you start firing, do not adjust your weapon.

5-41. When the decision is made to engage an aircraft with small arms, every weapon (M4, M240, M249, and M2) should be used with the goal of placing as many bullets as possible in the enemy's flight path. That does not mean that everyone fires in some random direction. Instead, everyone selects an aiming point in front of the UAS and fires at that point. This aiming point is determined using the football field technique. When deciding to fire upon an enemy UAS, practical considerations need to be considered before engaging. An example is engaging a UAS from a range of 3 kilometers. It is important to consider the capabilities of the available weapons. Using small arms at this range is ineffective while the best possibility may be the use

of the main gun on a tank or tracked vehicle. Small arms have a low probability of kill against attacking UAS due to their size, speed, and maneuverability.

Football Field Technique

5-42. The football field technique is a simple method of estimating lead distance. The theory is that most people have played or watched football and have a concept of how long a football field is. When told to lead the UAS by one football field, everyone aims at approximately the same point in space. One person's error in making the football field estimate will be offset by another person's error. The variation in aiming points will ensure that massed fire is delivered into a volume of space in front of the UAS rather than on a small point. Also, the differing perspectives from which the service members view the UAS will act to further distribute the fire over a volume of space.

5-43. Aiming points used to engage threat UAS are different but may be used on a variety of different threats. An example of this technique would apply if enemy helicopters were detected, and the decision was made to engage it should be engaged as a group 5 rotary wing UAS. The rules for selecting aiming points are simple, easily learned, and retained. The various aiming points are summarized in table 5-4.

Table 5-4. Aiming Points

<i>UAV Type</i>	<i>Course</i>	<i>Aiming Point</i>
Group 1 UAS	Crossing	0.5 football fields in front
Group 2 UAS	Crossing	1 football field in front
Group 3 - 5 UAS	Crossing	2 football fields in front
All UAS	Directly at you	Slightly above the UAS body
Rotary wing	Hovering	Slightly above the UAS body
<i>Legend</i>		
UAS unmanned aircraft system		

Engaging With Machine Guns

5-44. The machine gun is effective against slow-moving UAS. To sustain the volume of fire and kill a UAS, a continuous burst of 20 to 25 rounds fired using a tracer on target method, allowing the gunner to adjust rounds on target as follows:

- Vehicle's machine guns are useful weapons against UAS. They can be fired quickly unleashing a high-volume of fire. Ensure that the area is clear of friendly personnel. Use the following guidelines when using crew served weapons.
- When UAS are hovering or inbound, aim high with the machine gun and fire a continuous burst, adjusting onto the UAS by observing the travel and impact of tracers remembering, tracers may appear to be striking the target when they are going under it.
- If engaging a moving UAS, track along its flight path using a lead of 50 meters or half a football field. Fire a continuous burst, forcing the UAS to fly through the cone of fire.

5-45. When coordinated effectively, the aircraft will fly through the unit's cone of fire. Vehicle commanders must not try to track high-speed aircraft because they fly too fast. When enemy aircraft fly directly at vehicles, vehicle commanders are responsible for engaging them with controlled machine gun bursts of 50 to 100 rounds. Select an aiming point slightly above the nose to position the UAS in the cone of fire.

5-46. Due to the speed of some types of UAS, the best technique to use against them is to fire all automatic weapons in continuous bursts. If the UAS are inbound, aim slightly above the nose or fuselage and fire. If the UAS is crossing, use a lead of 200 meters (two football fields) and fire letting the UAS fly through the cone of fire from the machine guns. Do not try to track or traverse your fire for group 3 and above UAS since they fly too fast.

Chapter 6

Air Defense Warnings and Controls

This chapter describes how air defense warnings (ADWs), weapons control statuses, and ROE are used to mitigate the effects of potential air threats and attack. This chapter also addresses the execution phase of the Army's operation process presented in terms of engagement operations.

AIR DEFENSE WARNING CONDITIONS

6-1. Air defense C2 nodes distribute standardized air defense warnings (ADWs) to alert all forces of air and missile attacks. Commanders can issue local ADWs, which provide additional guidance alerting all members within their area of operations. Supported units may monitor the AMD early warning network that contains specific information for ADA units to include more detailed track information. However, the format of directed early warning does not necessarily follow the size, activity, location, unit, time, and equipment report format. Hostile track information and targeting data may be reported using the same systems as directed early warning. Frequencies used to monitor AMD early warning networks are located in the unit's communications plan.

6-2. ADW conditions demonstrate the degree of air attack probability based not only on current threat assessments but also on future air threats as required. The area air defense commander (AADC) issues ADWs for the joint operations area, based on current threat intelligence and disseminated through C2 channels to subordinate AMD commanders.

6-3. There are three types of ADWs: red, yellow, and white, with red being the most urgent. Any commander, after coordination and approval through air defense channels, may issue a higher level of warning for their command but may not lower the level. The chain of command must ensure that every Soldier knows the current ADW. ADWs will be disseminated through C2 systems throughout a theater. It is the responsibility of supported units at every echelon to inform their respective commanders of the current ADW. Army commanders must then inform their subordinate units of the ADW. See FM 3-01 for further discussion on ADWs. Descriptions of the ADWs are as follows:

- ADW red. An attack by hostile aircraft or missile is imminent or in progress.
- ADW yellow. An attack by hostile aircraft or missile is probable.
- ADW white. An attack by hostile aircraft or missile is improbable.

ALERT STATES AND READINESS CONDITIONS

6-4. AMD commanders use weapons alert designators, alert states and readiness conditions to ready their forces and configure their systems rapidly against an enemy air attack. An example of this is the ready for action drills conducted upon receiving a new surface to air missile tactical order, which heightens a unit's alert state. In conjunction with elevating the unit's readiness, the commander also retains the ability to stand down units for rest or maintenance.

6-5. Alert states and readiness conditions are implemented locally and coordinated with guidance from the AADC and designated controlling authorities. The combined arms force should understand ADA brigade commanders establish and control the alert state for their subordinate units operating in support of forces in the maneuver areas of operation. Actual timelines and manning requirements are determined by theater or joint operations area plans. Alert state and readiness condition information is normally found in the unit's tactical standard operating procedures which also considers the factors of mission, enemy, terrain and weather, troops and support available, time available, and civil considerations.

RULES OF ENGAGEMENT

6-6. *Rules of engagement* (ROE) are directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered (JP 3-84).

6-7. ROE at all echelons are positive and procedural directives that specify the circumstances and limitations under which forces will initiate or continue combat engagements with enemy forces. The joint force commander approves the theater ROE. These established ROE enable the commanders to delegate the authority to execute air defense operations.

6-8. ROE permit the senior air defense commander to retain control of an air battle by prescribing the exact conditions under which engagements may take place. ROE is a direct reflection of the centralized control with decentralized execution principles of air defense. ROE apply to all warfare participants in the theater and are disseminated to all echelons of air, land, and sea forces. There are seven AMD ROE categories: right of self-defense, identification criteria, fire control orders, weapons control status, levels of control, autonomous operations, and modes of control.

Right of Self-Defense

6-9. Commanders at all echelons must take whatever action is necessary to protect their forces and equipment against air attack, to include from UAS. Self-defense operations allow friendly units to defend themselves against direct attacks or threats of attack with the use of organic weapons and systems.

6-10. When under attack, the right of self-defense takes precedence over any other established rules and procedures, which normally govern engagement. The right of self-defense is inherent in all ROE and weapons control procedures (JP 3-01).

Identification Criteria

6-11. The employment of C-UAS systems requires early identification of friendly, neutral, or hostile UAS to maximize effective range engagement. Active defense measures protect the force, reducing delays during tactical operations, and mitigate fratricide. Positive identification of aircraft is normally the preferred method of operation. Positive identification is an identification derived from observation through visual recognition, electromagnetic support systems, identification friend or foe systems, or other physics-based identification techniques. In the absence of positive identification, procedural identification is used, which employs previously established and disseminated airspace coordinating measures. Procedural identification separates airspace users by geography, altitude, heading, time, and/or maneuver. Generally, some combination of positive and procedural identification will be used. For more information refer to FM 3-01.

6-12. Proper employment of air defense weapon systems enables early detection, identification, classification, and alert of threat aircraft and missiles which maximizes beyond-visual-range engagements and helps to avoid fratricide. Identifying and classifying friendly air platforms from enemy assets while employing various weapon systems is a highly complex task. For example, visual identifications may be different from identifications provided earlier by alerting sensors and supporting systems. Additional considerations include time of detection, range, projected flight path, and possible battlefield effects. Tasks will differ based on the type of threat platform detected, whether manned or unmanned. While the ROE for aircraft may allow additional time before engagement, this will not always be the case with UAS.

6-13. Hostile criteria are basic rules that assist in the identification process of friendly or hostile air platforms. These rules are promulgated through subordinate commanders from the joint force commander or AADC when so authorized. The commander who establishes hostile criteria parameters may consider the factors of speed, altitude, and heading or other requirements within specified volumes of airspace. The local commander may also consider specific enemy threat characteristics or hostile acts.

6-14. Echelons having engagement authority use hostile criteria to determine the identification of detected air targets. The highest echelon capable of managing engagement operations normally retains identification and engagement authority. Upon target detection, fire units and sensors with real time and near-real-time data transmission capability assist the controlling authority by forwarding targeting information. The controlling authority makes the final target identification and delegates engagement authority. Engagement authority may be given to the lowest echelon, such as a crew, capable of directing an engagement, depending upon such factors as the type, intensity, and area of operations of the air threat.

Fire Control Orders

6-15. Fire control orders are commands used to control engagements on a case-by-case basis, regardless of the prevailing weapon control status. Higher ADA echelons, when monitoring the decentralized operations of subordinate units, most often use these commands. Fire control orders can be transmitted electronically or verbally; however, not all the fire control orders shown below can or will be used by every type of ADA unit. The orders most applicable to C-UAS operations are-

- *Engage*. In air and missile defense, a fire control order used to direct or authorize units and/or weapon systems to attack a designated target. (JP 3-01) Engage is an order issued by the engagement authority.
- *Hold Fire*. An emergency fire control order to stop firing on a designated target and destroy missiles in flight (ATP 1-02.1).
- *Cease Engagement* or *Cease Fire*. A fire control order used to direct air defense units to stop tactical action against a specified target. Missiles in flight will continue to intercept (ATP 1-02.1).

Weapons Control Status

6-16. A *weapon control status* is an air and missile defense control measure declared for a particular area and time by an area air defense commander, or delegated subordinate commander, based on the ROE, that establish conditions under which fighters and surface air defense weapons are permitted to engage threats (JP 3-01). Weapon control status establishes procedures for forces using surface air defense weapons (including small arms weapons) to engage threats. Weapon control statuses can apply to weapon systems, volumes of airspace, or types of air platforms. The tactical situation normally determines the degree or extent of control necessary over particular weapon systems. ADA officers at headquarters planning cells or AMD coordination and liaison teams typically establish or recommend separate weapon control statuses for various air threats, including fixed and rotary-wing aircraft, or UAS, at their supported headquarters. Air defense is optimized when all forces have the ability to rapidly receive and disseminate weapon control statuses for all air platforms. The three weapon control statuses are:

- *Weapons free* is the least restrictive status: used to indicate when any target not positively identified as friendly in accordance with current ROE may be engaged (JP 3-01).
- *Weapons tight* is the normal status. Units may only fire on targets identified as hostile in accordance with current ROE (JP 3-01).
- *Weapons hold* is the most restrictive status. Units may only fire in self-defense or when ordered by proper higher authority (JP 3-01).

6-17. Any unit can receive ADW or directed alert of possible or immediate threats to their forces or to a specific area of the battlefield. The AMD cell provides the air defense expertise for integration into the corps/division air defense plan. The ADAM personnel contribute to the brigade and below units' airspace plans. The airspace control element reviews and deconflicts the corps or division air defense plan with other division control measures. The control measures for the air defense plan are normally sent to higher headquarters through AMD channels.

Level of Control

6-18. Level of control describes the ADA echelon at which positive management of the air battle is conducted. This can be an AADC, regional air defense commander, sector air defense commander, ADA brigade, battalion, or the individual unit. Different levels of control are normally established for engagements of fixed-wing aircraft, rotary-wing aircraft, and UAS.

Modes of Control

6-19. Combined arms forces must be familiar with the overall area air defense plan that specifies the modes of control, trigger events and when they should be changed, and who has the authority to change them. The mode of control selected may depend upon the capabilities of the communications system, the weapons systems employed, and both the friendly and enemy air situations. There are three modes of control in AMD: centralized, decentralized, and autonomous. (For more information on each refer to FM 3-01.)

- Centralized control mode. In this mode, a higher echelon must authorize target engagements by a firing unit.
- Decentralized control mode. In this mode, a higher echelon monitors unit actions and makes direct target assignments on a management by exception basis, to ensure proper fire distribution, prevent engagement of friendly air platforms, and prevent simultaneous engagements of hostile air targets.
- Autonomous operations. A unit assumes autonomous operations after it has lost all communications with higher and adjacent echelons. The unit commander assumes full responsibility for control of weapons and engagement of hostile targets. Normally, the ROE and supplemental fire control measures in effect at the time of communications 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 will be implemented as scheduled.

EXECUTION

6-20. Ground-based or aerial sensors, or combinations of both when available, are employed to perform surveillance of the airspace and provide focused early warning to at-risk forces. The sensors provide engagement authorities the time to make engagement decisions that deny threat platforms the ability to see or impact the defended assets.

6-21. These engagement authorities function as a vertically and horizontally integrated kill chain. The kill chain is the successive linkage of commanders who can authorize engagements of air and missile threats (FM 3-01). The designated engagement authority in the kill chain, providing operational control of and, ultimately, directions to the shooter, makes engagement decisions. Integrated sensors, shooters, and C2 networks will allow for greatly increased engagement options. As such, engagement authorization must be delegated to the lowest level possible.

6-22. Proactive engagements are conducted in accordance with theater-level ROE and complementary directives. The best shooter-that weapon system that can best deliver the appropriate effects to achieve maximum attrition at the right time and place, and as far forward as possible, to ensure keep-out ranges and keep-out altitudes-conducts engagements. Keep-out range is the horizontal distance from a defended asset at which a successful engagement denies an adversary's desired weapons effects against the defended asset. It also allows C-UAS systems to counter enemy aerial surveillance and reconnaissance platforms beyond the range at which they can surveil an asset and beyond the engagement capability of a defending AMD system, contributing to the overall ability of friendly forces to see first. Keep-out altitude is the vertical distance above a defended asset at which a successful engagement denies an adversary's desired weapons effects against the defended asset. The method of fire may be stipulated in operation plans, directed by the kill chain, or influenced by the situation. Coordination is affected by the AMD C2 elements to ensure the AMD weapons, facilitating their destruction while simultaneously mitigating the potential for fratricide of friendly and neutral aircraft, overmatch the threats.

6-23. Maneuver forces using C-UAS systems can provide vital protection from UAS, thereby contributing to freedom of maneuver. The C-UAS systems enable maneuver forces to effectively detect and engage UAS at ranges and altitudes that deny them surveillance and attack options. Stinger teams organic to maneuver formations further enhance this capability. The ADAM cell in the maneuver brigade links the maneuver forces to the kill chain to implement appropriate ROEs. Intelligence enables cyber and EW elements to electromagnetically attack air targets. Intelligence elements can also provide or assist in the surveillance, identification, and classification of air targets, facilitating early warning. For more information refer to FM 3-0 and ATP 3-01.8.

Chapter 7

Sustainment Training

Training to counter the UAS threat is critical to preparing Army forces to succeed on the modern, evolving battlefield. This appendix includes discussion regarding the delivery of material, non-material, and training required to prepare the force to apply appropriate protective measures and materiel solutions to succeed against an agile and adaptive enemy.

OVERVIEW

7-1. The threat posed from UAS employed by our adversaries has, and likely will continue, to increase at a rapid pace. Technology advances and capabilities in commercial-off-the-shelf UAS make it extremely easy for threat actors to employ these commercial-off-the-shelf systems to accomplish their goals. These platforms can easily be modified to carry payloads creating impacts that are even more devastating. In addition, nation states are developing military grade UAS that have even greater threat capabilities. Continual improvement of C-UAS training is paramount to enable U.S. forces to organize, plan, and conduct C-UAS activities; properly employ C-UAS equipment; and better understand and UAS threats.

7-2. Commanders and staffs must continually identify problems or issues related to current and future doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy that affect mission accomplishment. As commanders and staffs identify issues; analysis is required to determine what actions or coordination should take place to resolve the issue. Identified issues and requirements that cannot be resolved internally should be passed on for assistance outside the command.

7-3. Rapid development, acquisition, and fielding of C-UAS solutions, synchronized across doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy to address operational requirements in the field, requires a deliberate effort. The Army proactively identifies and analyzes C-UAS capability gaps to develop, train, and employ solutions to counter the threat. The Joint C-UAS Office has been established to execute C-UAS Executive Agent responsibilities for the Army to synchronize C-UAS efforts across all services within Department of Defense. The Joint C-UAS Office operates as a central hub for collecting identified requirements and coordinating, synchronizing and integrating C-UAS training, doctrine, materiel and policy solutions.

7-4. To accomplish the task of synchronizing and executing development and implementation of C-UAS requirements, several key areas should be addressed:

- Identifying operational needs.
- Collecting observations, insights, and lessons leading to development and assimilation of lessons learned.
- Provide relevant C-UAS training across all three training domains (self-development, institutional, and operational).

IDENTIFYING OPERATIONAL NEEDS

7-5. Commanders drive change by identifying opportunities for adaptations, choosing solutions, and integrating those solutions into their organizations. Commanders identify the need for change using unit-generated and Army- or joint-approved operational needs statements (ONSs) as requirement documents. (See AR 71-9 and TRADOC Reg. 71-20 for additional information on capabilities determination.)

7-6. An ONS identifies and characterizes gaps in existing capabilities that are significant obstructions to achieving mission objectives. Commanders use an ONS to document an urgent need, correct a deficiency, or improve a capability that enhances mission accomplishment. Additionally, the ONS provides an opportunity for commanders outside the acquisition, combat development, and training development communities to initiate the capability determination process.

7-7. An ONS is often the initial step toward a new development or a process improvement program. Commanders and their higher headquarters conduct a needs assessment to determine the best capabilities U.S. forces will require to accomplish mission tasks. The ONS is not a Joint Capabilities Integration and

Development System capability document, but it is a request for requirement validation and sourcing of a perceived requirement. Commanders cannot use an ONS to request or redistribute standard authorization, documented shortages (such as items identified in a modified table of organization and equipment, table of distribution and allowances, or mission-essential equipment list) or previously validated deployment items.

7-8. Responses to a command submitted ONS vary depending on the priority of need for the required capability. The ONS will be returned to the originator if TRADOC determines that there is not a valid operational need (requirement). If TRADOC validates the operational requirement, it may approve the request for sourcing execution through the acquisition process, direct the transfer of pre-positioned equipment, or take no action until additional analysis is complete.

7-9. Commanders submit an ONS through their operational chain of command. Commanders should refer to published guidance from higher headquarters for submitting an ONS when technology systems are unavailable.

Collecting Observations, Insights, and Lessons

7-10. Observations, insights, and lessons are information from any source that explains the conditions experienced by U.S. forces during war or training, the issues that arose during those military operations or exercises, and the potential solutions to the issues. The TTP, after action reviews, operational records, and lessons learned from actual Army operations, experiments, and training events contribute to the development of observations and insights. The collection of observations, insights, and lessons learned is part of the overall lessons-learned process. (See AR 11-33 for detailed discussions of the Army Lessons-Learned Program.)

7-11. Commanders use formal and informal means to collect relevant observations, insights, and lessons; after action reviews; and other documentary materials that support the creation of lessons-learned products. Formal (direct or active) collection involves the use of subject matter experts during military operations and exercises. These teams use a prepared and approved collection plan to focus and prioritize efforts. Observers document, organize, and collect records and after action reviews and provide feedback to the units they are observing. Informal (indirect or passive) collection occurs when units or individuals submit operation, exercise, training, or rotation after action reviews.

7-12. Doctrine-based after action reviews identify strengths and shortcomings in unit planning, preparation, and execution and guide leaders to accept responsibility and develop solutions for the identified shortcomings. Commanders determine how to improve effectiveness by analyzing the data. Commanders submit their C-UAS after action reviews and other lessons to the Center for Army Lessons Learned for additional analysis, archiving, and dissemination to the Army and the C-UAS community of practice.

7-13. The analysis process organizes and evaluates information with the purpose of determining its meaning, elements, relationship, and relevance. Analysis identifies best practices that can be shared with U.S. forces; reveals capability gaps; and influences C-UAS training requirements, potential doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy changes, and capability development.

Developing and Assimilating Lessons Learned

7-14. Lessons learned are validated knowledge and experience derived from observations and the historical study of military training, exercises, and combat operations that lead to a change in behavior. Observations, insights, and lessons are not lessons learned until the assigned Army proponents validate them and there is individual, unit, or Army behavior changes. A change in behavior implies changes at the strategic, operational, or tactical (standing operating procedures/TTP) level or in one or more of the Army doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy domains. The purpose of collecting, identifying, analyzing, disseminating, and integrating lessons learned, critical information, and knowledge is to sustain, enhance, and increase the Army's preparedness to conduct military operations.

7-15. Not all solutions require doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy changes. As part of the learning process, commanders identify changes that they can directly make and those that require higher-echelon assistance. Commanders adjust their unit standing

operating procedures and TTP where possible to adapt to the unique aspects of the OE. Even minor unit changes can offer valuable insight to commanders and units who will deploy forces under similar conditions. Thus, commanders should document, disseminate, and archive their lessons learned products.

TRAINING

7-16. The Army trains to fight and win—it is what we do in order to preserve the peace and to decisively defeat our enemies. We do this through challenging, relevant, and realistic training performed to the highest standards. The Army trains the way it operates. It does this by replicating in training how we expect to fight, closing the gap between operations and training (FM 7-0). Leaders, Soldiers, and units achieve tactical and technical competence while building confidence and agility. U.S. forces train using doctrine that sustains their tactical and operational capabilities. Throughout this training, commanders treat UAS threats as a condition on the battlefield with an understanding that the UAS threat is inherent across the range of military operations and may be present in any location where U.S. forces operate.

Providing Relevant C-UAS Training

7-17. The training and development of leaders and Soldiers in any organization requires implementation of informed and proven training strategies to achieve success. Commanders provide vision, focus, direction, and an action plan in the development of training strategies. A commander ensures that the organization is trained and mission-ready by actively engaging in all aspects of training and integrating C-UAS capabilities, resources and activities into training.

7-18. Training time is always a premium. Relevant C-UAS training will likely never be conducted as a stand-alone training event within the context of collective and combined arms training. Rather C-UAS will largely be trained in terms of reacting to a threat or condition that is threaded throughout planned training.

7-19. It should be adaptive if it is to meet training requirements while balancing resource and time constraints. The training of combined arms C-UAS tasks requires planning and execution that begins at the lowest possible level. Commanders may face time constraints, resource limitations, and schedule conflicts in their efforts to achieve optimal training results. The ability to incorporate and sustain organizational capabilities depends on the quality of modernization and sustainment training. Commanders should tailor training and education with relevant information based on lessons learned, enemy trends, and friendly C-UAS TTP to ensure that the training meets the commander's intent and results in the unit being mission ready.

Leaders and Individual Training

7-20. The Army develops leaders to solve problems. Adaptive leaders are those who have a feel for the fight, who possess the ability to read the situation, and who can analyze the cause-and-effect relationships from the beginning to the end of an operation. An adaptive leader can translate operational and mission variables into situational understanding, is willing to accept prudent risk, and is able to make rapid adjustments based on knowledge assessments. In the modern fight, expanded access to information has compressed response times, resulting in squad level tactical actions that have immediate and lasting strategic consequences. The result is the need for adaptive leaders at the lowest echelon of U.S. forces.

7-21. The adaptive-leader skills that a commander develops and brings to the fight are the critical determinants in effectively applying combat power. Leaders improve their ability to adapt through knowledge and experience that is gained from multiple, complex, and unexpected situations in challenging, unfamiliar, and uncomfortable conditions. Commanders should address small-unit problem solving as a centerpiece of instruction based on relevant operational challenges. Leaders should gain the knowledge and experience necessary to think adaptively and critically. Outcome-based training developed by commanders should stress the philosophy of mission command for leaders (provide intent) and their subordinate leaders (determine how to achieve that intent).

7-22. Unit leaders must be able to understand the OE and apply C-UAS capabilities and measures within an overall protection framework. This includes employing and enforcing survivability measures and layered defense techniques in the employment of C-UAS capabilities. They must understand and adopt TTP for supporting friendly networks, influencing neural networks, and neutralizing threat networks. This requires training in nontraditional areas. Commanders should also integrate C-UAS activities and capabilities during

home station training and focus on integrating collective tasks that plan, coordinate, and control those capabilities.

7-23. There are several resources for C-UAS training. These resources support commanders in training individual level C-UAS skills and enable the development of C-UAS crew training. Most C-UAS training resources can be found on the Joint Counter-small UAS Office Community page housed on the Joint Knowledge Online portal. A list of C-UAS training resources that are available can be found in table 7-1.

Table 7-1. Counter-Unmanned Aircraft System Training Resources

C-UAS Training Resources	
Source	Description
Joint Knowledge Online C-UAS Community Page (https://jkodirect.jten.mil/Atlas2/page/desktop/DesktopHome.jsf)	A repository of material and links to online training developed by the Joint C-UAS Office. To access: go to the JKO Online portal at: https://jkodirect.jten.mil/ Login using government issued common access card (CAC). Go to "Community" on the gray banner at the top of the page. Select "Joint C-UAS Office"
JCO Policy Training Module (https://intelshare.intelink.gov/sites/JCO/Shared%20Documents/1_JKO%20Policy%20Training%20Module)	The JCO Policy Training Module provides instructions for DOD planners and leaders on policies, authorities, and authorized actions that affect C-UAS and UAS procedures, planning, and operations.
Joint C-UAS University (JCU) at Fort Sill, OK	The JCU currently offers three distinct courses: 1. Installation C-UAS Protection Course 2. Joint C-UAS Planner Course 3. Joint C-UAS Operator Course
Center for Army Lessons Learned (CALL) (https://call2.army.mil/)	Repository for Army lessons learned as well as observations, insights, after action reports, etc.
Joint Lessons Learned Information System (JLLIS) (https://www.jllis.mil/apps)	Repository for joint lessons learned as well as observations, insights, after action reports, etc.
Joint Knowledge Online C-UAS Training Modules	Training modules developed by the Joint C-UAS Office to basic C-UAS training for individuals.
Basic counter-small unmanned aircraft systems (C-UAS) Awareness Training. CAC controlled access. (https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=JCUAS&course_number=A-US1401)	Basic counter-unmanned aircraft systems (C-UAS) Awareness Training provides a basic awareness of general UAS threats, types and categories of UAS, and basic reporting requirements. This module is a prerequisite for all other C-UAS modules on JKO.
Basic counter-small unmanned aircraft systems (C-UAS) Familiarization Training. CAC controlled access. (https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=JCSUAS&course_number=A-US1402)	Basic counter-unmanned aircraft systems (C-UAS) Familiarization Training provides a review of the basic UAS awareness and an overview of select C-UAS systems and capabilities.
Basic counter-small unmanned aircraft systems (C-UAS) Installation Training. CAC controlled access. (https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=JCUAS&course_number=US1403)	Basic counter-unmanned aircraft systems (C-UAS) Installation Training provides a threat overview, information on policies and authorities associated with UAS and counter UAS operations at installations and fixed sites, planning considerations, and reporting procedures.
Basic counter-small unmanned aircraft systems (C-UAS) Tactics, Techniques, and Procedures (TTP). CAC controlled access. (https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=JCUAS&course_number=US1404)	Basic counter-unmanned aircraft systems (C-UAS) Tactics, Techniques, and Procedures (TTP) provides an overview of the threat and operational environment, general TTP for C-UAS, reporting procedures, and select UAS case studies.
For Counter-Small Unmanned Aircraft Systems (C-sUAS) Policy Training. CAC controlled access. (https://jkodirect.jten.mil/html/COI.xhtml?course_prefix=JCSUAS&course_number=US1405)	The Policy Training Module is a C-sUAS and UAS Policy training tool and reference developed for all Services' C-sUAS leaders, planners, and operations personnel.
https://www.faa.gov/UAS/commercial_operators/become_a_drone_pilot	To fly a drone under the FAA's Small UAS Rule (Part 107), you must obtain a Remote Pilot Certificate from the FAA. This certificate is needed if running a C-UAS range off military installation.

C-UAS Crew Training

7-24. There is a significant amount of C-UAS employed within operational theaters and being developed to become programs of record. Many of these systems are complex system-of-systems capabilities. Commanders of units being equipped with these systems must assess manning requirements for the capability and ensure all operators are adequately trained on the systems. In some cases, crews must be identified, trained and certified to effectively employ these capabilities. Commanders must—

- Identify crew size/composition.
- Develop/train crew drills.
- Certify crews to employ the C-UAS capabilities.

7-25. Certified crews should be incorporated into unit collective training whenever possible to maintain crew proficiency and ensure the C-UAS mission is fully coordinated, integrated, and synchronized into operations and all relevant staff elements such as targeting cells, ADAM/BAE, intelligence, protection, and CEMA.

Combined Arms Training

7-26. Commanders focus on critical skills in combined arms training that enable rapid adaptation to the challenges of specific missions and conditions. Those conditions include incorporating realistic battlefield noise, obscurity, loss of key leaders, casualties, limited visibility (night), force-on-force training with an uncooperative enemy force (civilian and media role players), and a variety of terrain. C-UAS will rarely if ever be a stand-alone mission for commanders across the force. Rather, the C-UAS effort must be thought of and trained as a condition of the battlefield. This enables commanders and trainers to thread C-UAS events into existing training. This lessens the overall impact of obtaining limited training time for C-UAS at the collective level. Commanders, subordinate leaders, and any Soldiers or crews assigned C-UAS missions should experience the stressful, near-combat training environment provided at home station and combat training centers.

7-27. Where possible, leaders leverage specifically designed training aids, devices, simulators, and simulations to enhance collective task training in the defeat and mitigation of C-UAS threats. Simulations enable adjustments to battlefield C-UAS conditions, ranging from experienced to less experienced training audiences. These training aids, devices, simulators, and simulations devices can be used to train individuals and crews. Training aids, devices, simulators, and simulations devices can be incorporated into collective training to train commanders and staffs during large-scale, highly compressed training events, thus forcing attention on decision making.

7-28. Commanders should leverage training opportunities at the various combat training centers. Combat training centers may also be a source for C-UAS TTPs, and lessons learned and facilitate the development, fielding, and testing of new equipment, training, and concepts to enable C-UAS efforts. Commanders are encouraged to contact the combat training centers before home station training events to aid in integrating joint capabilities and new technologies.

Refining Training Requirements

7-29. Commanders and leaders should understand the nature of organizational change to execute planned and programmed force integration actions. They should be able to assimilate change effectively and efficiently to maintain combat-ready units. Training is cyclic, and the results are perishable. The pace of technological change fluidity of the UAS threat demands a systematic TTP and lessons learned validation and integration approach.

7-30. Figure 7-1 on page 64 represents a sample methodology for updating C-UAS training concepts, strategies, and tasks. Techniques within the methodology depict a flexible approach that allows nearly immediate critical C-UAS observations, insights, lessons learned, and enemy TTP information sharing. The methodology begins at the tactical level and concludes with the identification and implementation of enduring principles in the institutional training domains.

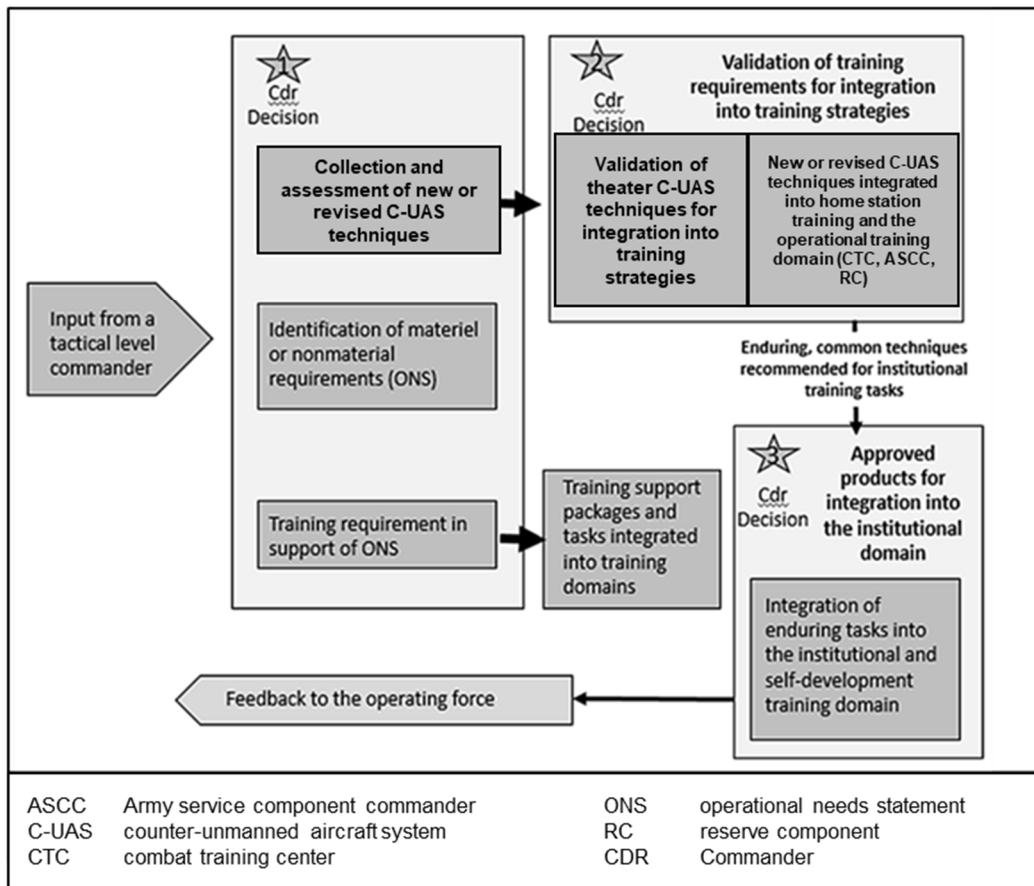


Figure 7-1. Counter-unmanned aircraft system training update methodology

7-31. This methodology ensures the disciplined validation and integration of best practices, enemy TTP, and lessons learned across the three training domains—operational, institutional, and self-development. More importantly, this methodology recognizes that training requirements, courses, and capabilities will evolve and change as the threat adapts and new training and materiel solutions are developed. This training update methodology includes—

- Identification of requirements. The methodology begins with the identification of requirements at the tactical level. Commanders submit an ONS, resulting from the collection and assessment of new or revised TTP, enemy TTP, or identification of materiel or nonmaterial requirements.
- Validation of training requirements for integration into training strategies. Commanders validate and integrate the training information into the operating-force training strategies as a means of further developing leader, Soldier, and unit abilities. The integration of the training information also involves applying previously learned individual and collective task skills in scenarios that are more complex and situations. Training progression starts with home station training, progresses to the unit validation training event (such as a mission readiness exercise at a combat training center or at a mobilization training center), and continues with deployment.
- Integration of approved products into the institutional training domain. Tasks deemed as enduring become approved products for integration into the training domains. In some cases, enduring tasks are integrated into the institutional and self-development training domains. The institutional training domain provides a strong foundation (based on tested and proven essential tasks) that Soldiers and leaders build on for success in the OE. Institutional training on C-UAS tasks includes common tasks and branch-specific training across the Army. Leader, Soldier, and staff common tasks capture the basic tactical expectations for each group. TRADOC implements these common tasks at all levels of Army institutional training.

- Assimilation and feedback to the operating force. Feedback to the operating force on respective changes in the three training domains allows for greater and quicker adaptation. The implementation of common tasks and feedback also creates additional training time for commanders who are no longer required to train the common tasks.

7-32. Training and leader development are tools that force integrators use to incorporate and sustain new capabilities in organizations based on changes in concepts, doctrine, organizational structure, and materiel systems. Commanders should periodically review the directed, mission-essential task list; changes in enemy TTP; or new C-UAS equipment and capabilities to sustain or retrain certain tasks as required.

This page intentionally left blank.

Appendix A

C-UAS Equipment

The systems within this appendix represent some of the most common capabilities currently fielded operationally to address the UAS threat. Air defense personnel employ some of these systems while some are operated as branch agnostic capabilities. This is not an all-inclusive list but represents the most common systems currently in use across Army theaters.

FIXED SITE-LOW, SLOW, SMALL UNMANNED INTEGRATED DEFEAT SYSTEM

A-1. The Fixed Site-Low, Slow, Small, Unmanned Integrated Defeat System (FS-LIDS) is an integrated C-UAS system-of-systems that can detect, identify, track and defeat UAS threats (see figure A-1 on page 68). The FS-LIDS employs an EW capability, via the Duke and direction finding antennas, to provide improved detection and defeat probability. It uses an electro-optic/infrared camera with automatic slewing capability working with radar to capture and track the target for positive identification. The major subsystems of the FS-LIDS include-

- EW subsystem. Major components include-
 - A primary unit.
 - A secondary unit.
 - An EW position, navigation, and timing element.
 - A low noise amplifier.
 - C2 laptop.
 - A direction-finding unit.
 - A C-kit mast.
- Radar subsystem. Major components include-
 - Central antenna assembly.
 - Top hat assembly.
 - Antenna columns.
 - Inertial navigation system.
 - Scope assembly.
 - Ground planes.
 - Power supply.
- Camera subsystem. Major components include-
 - Infrared camera.
 - Electro-optical camera.
 - Positioner.
 - Electronics box.

A-2. An AN/TPQ-50 multi-mission radar actively detects and tracks UAS while the Nighthawk electro-optical infrared camera and the Counter-Unmanned Aircraft Electromagnetic Warfare System provides secondary location, verification, identification, and classification of detected UAS. The Counter-Unmanned Aircraft Electromagnetic Warfare System suite defeats UAS threats through its EA capability to disrupt or jam threat UAS position, navigation, and timing, command link, and video downlink signals. The FS-LIDS has lethal capability when coupled with the Coyote family of UAS interceptors.

A-3. The Forward Area Air Defense Command and Control system provides engagement operations, aircraft avoidance, and fratricide prevention. Forward Area Air Defense Command and Control system enables air defense C2 system interoperability with Link-16.

A-4. FS-LIDS equipped with a lethal defeat solution includes a palletized KuRFS radar and a palletized Coyote missile pod (see figure A-2 on page 69).

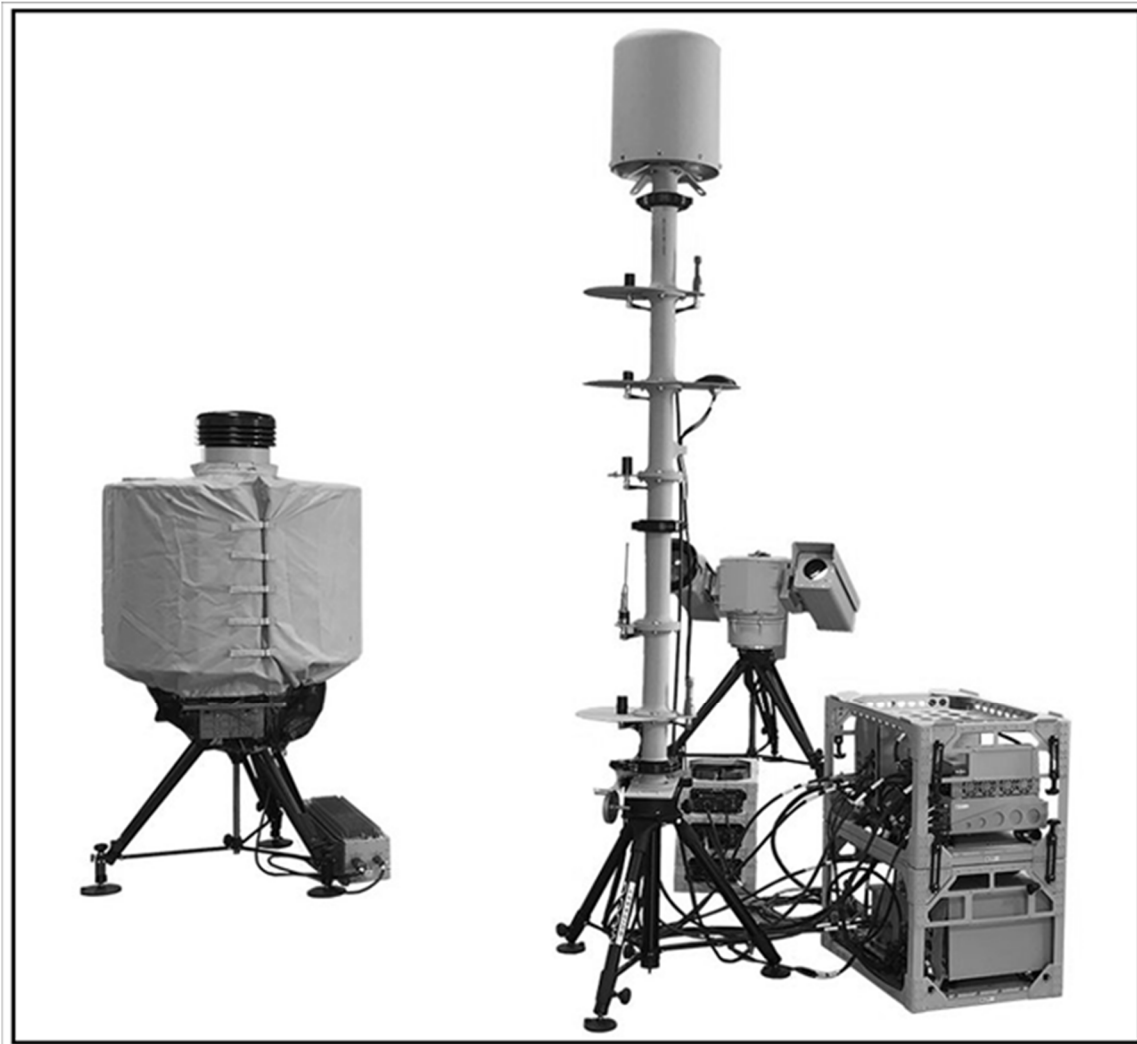


Figure A-1. FS-LIDS



Figure A-2. FS-LIDS kinetic defeat solution

KU-BAND FUNCTION RADIO FREQUENCY SENSOR

A-5. The Ku-Band Multi-Function Radio Frequency System (known as KuRFS) is a proven, true multi-mission radar capable of providing simultaneous C-UAS, counter-rocket, artillery, and mortar (C-RAM), air surveillance and effector support missions that can be either mobile or palletized (see figure A-3 on page 70). The KuRFS radar provides target tracks for all categories of UAS and can discern air targets from ground targets. KuRFS provides sensing and fire control capability, delivering a clear air picture and improved probability of kill across an array of effectors, including the high energy laser (HEL) and EW effectors, and lethal-defeat missiles and guns for C-UAS such as the Coyote Weapon System, 50-caliber guns, 30-millimeter cannons, the Land-based Phalanx Weapon System (LPWS).

A-6. The KuRFS is designed to support growth and adaptation to the evolving threat environment.

- Simultaneous, multi-mission capability providing low-cost SHORAD solutions.
- Searches the entire upper hemisphere.
- Provides clear, actionable air picture, filtering biological entities, small arms fire and ground vehicles; minimizes false alarms.
- Remotely operated by the C2 operator.
- Precision fire control capability extends weapon system and effector capabilities.
- Precision real time track adaptation for low-priced lethal defeat effectors, like Coyote.
- Enables defense against multi-axis, multi-threat attacks.

A-7. The KuRFS radar family consists of two options:

- The palletized radar is intended for fixed sites and can be packaged on a medium tactical vehicle class for transportable capability to remote and temporary locations. The palletized radar enables SHORAD/C-UAS protection of high-value assets and military facilities.
- The mobile configuration of the KuRFS, which fits within the size, weight and power limits of a mine resistant ambush protection all-terrain vehicle, joint light tactical vehicle or other light tactical vehicle. The mobile radar provides the range capability to support light expeditionary and small mobile unit operations.



Figure A-3. Ku-Band Radio Frequency System (KuRFS)

COYOTE BLOCK 2C

A-8. The Coyote Block 2C is an expendable, rail/tube launched, turbine engine-powered missile for high-speed C-UAS missions (see figure A-4). It is a ground-to-air effector proven against small maneuvering UAS threats with rapid time-to-target. It is command and control guided to target using KuRFS family of radars until the onboard seeker takes over for terminal engagement. Destruction of the UAS is completed with detonation of the low collateral damage, forward-firing blast fragmentation warhead. The KuRFS enables surveillance of the airspace near the Coyote Block 2C launcher to allow operators to verify that airspace is clear of friendly platforms.

A-9. Coyote Block 2C is integrated into both fixed site and mobile platforms for flexibility of mission employment. It can be ground launched, or vehicle mounted. The ground launch configuration is one 4-pack launcher; the mounted version is one two-pack launcher. Integration with Forward Area Air Defense Command and Control allows engagement of multiple targets, with multiple Coyote Block 2C warheads simultaneously.

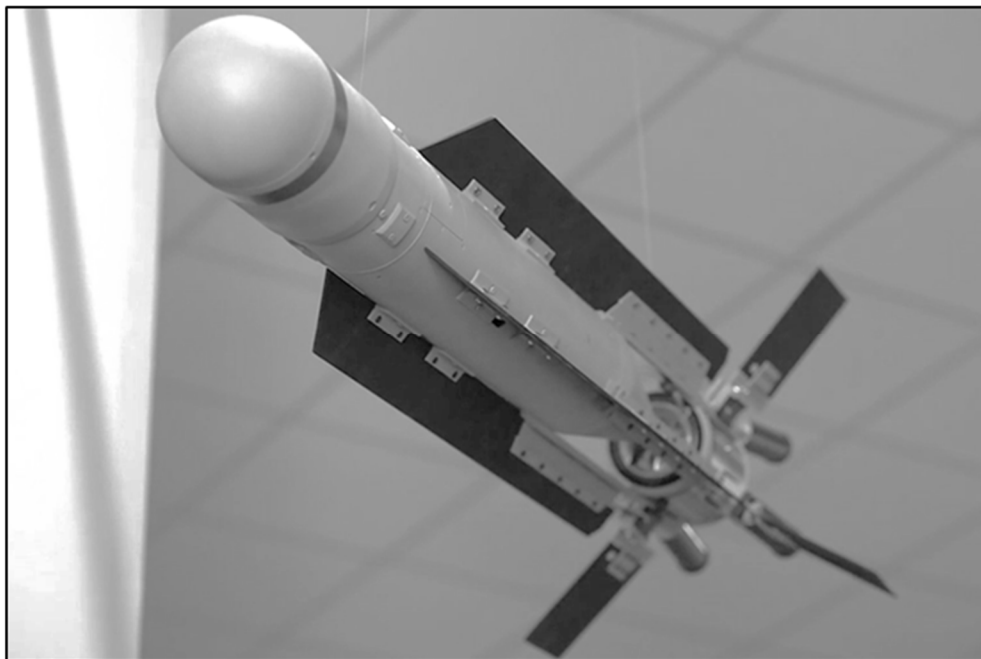


Figure A-4. Coyote Block 2C

COUNTER-REMOTE CONTROL MODEL AIRCRAFT INTEGRATED AIR DEFENSE NETWORK (CORIAN)

A-10. The Counter-Remote Control Model Aircraft Integrated Air Defense Network (known as CORIAN) is a C-UAS system that can detect, identify, track and defeat threat UAS (see figure A-5 on page 72). The system is configured with multiple EW capabilities enabling non-lethal engagements. The system consists of passive and active sonar nodes for detection, geolocation and disruption of UAS in its target library. The CORIAN system-

- Provides continuous, automated monitoring in all weather conditions.
- Recognizes and tracks UAS radio links to identify and locate UAS operating in restricted or protected airspace.
- Can locate UAS ground control stations.
- Passive sensors-
 - Detect and geolocate targets in a 360-degree field of view.
 - Create an electronic perimeter detection boundary.
 - Provide time-difference of arrival geolocation information based on sensor data collected by three or more sensors and displays probability ellipses on the graphic user interface map.
- Active Sensors-
 - Disrupt non-Wi-Fi targets by attacking C2 uplinks and targeting RF bands.
 - Can attack a single target or jam a wide area depending on type of attack +-initiated.

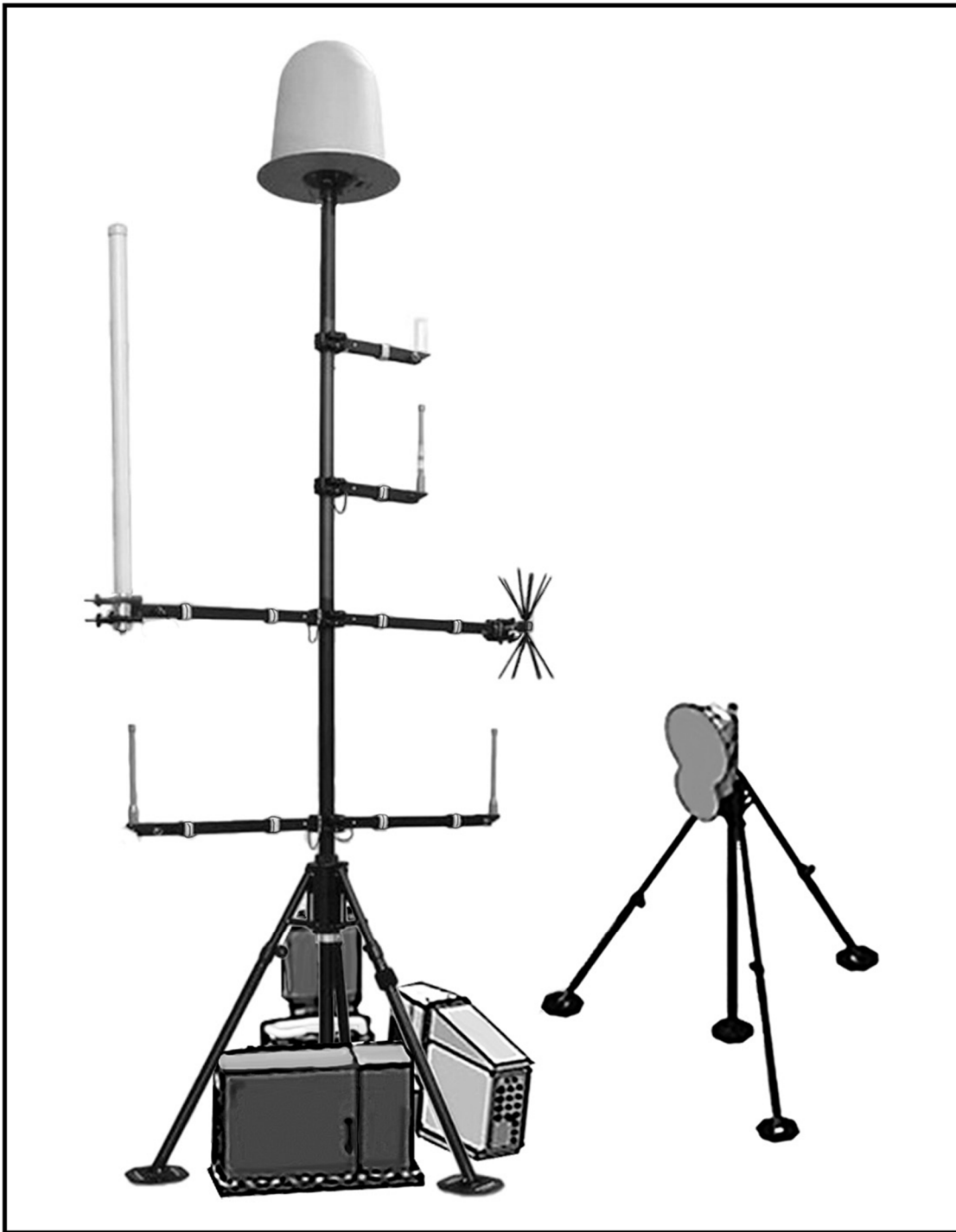


Figure A-5. Counter-Remote Control Model Aircraft Integrated Air Defense Network (CORIAN)

NEGATION OF IMPROVISED NON-STATE AERIAL-THREATS (NINJA)

A-11. The Ninja is a C-UAS system that can detect, identify, track and defeat threat UAS using a library based, RF capability (see figure A-6). The Ninja disrupts threat UAS communications through RF detection, tracking and EA. The Ninja-

- Passively detects, identifies, and tracks UAS.
- Actively defeats hostile UAS without indiscriminate interference to friendly systems.
- Enables multiple defeat options depending on threat signal protocols.
- Can operate as a stand-alone system or networked with other Ninja nodes, compatible electronic jammers (EGON, DRAKE, Duke), or autonomous interceptors.
- Ninja also has a mobile variant (Ninja Transmit and Receive) and a dismounted variant (Ninja Manpack).



Figure A-6. Negation of Improvised Non-State Aerial-Threats (NINJA)

ANVIL

A-12. Anvil is a quadcopter that when cued by the system, navigates autonomously to intercept potential threat UAS. It provides visual feedback to the operator, employing artificial intelligence (AI) and computer vision technology, to obtain positive identification. Once authorized, the Anvil uses physical speed and onboard terminal guidance to deliver lethal effects to the threat with minimal collateral damage (see figure A-7 on page 74).



Figure A-7. Anvil

WINDTALKER

A-13. The Windtalker system provides warfighters the ability to detect, identify and track DJI devices. It provides long-range detection of DJI aircraft and associated ground control stations and can identify whether the UAS is transmitting a valid identification, friend or foe IFF code (see figure A-8).

A-14. It is easy to operate and low maintenance. The system user interface can provide situational awareness across multiple sensors through a cloud-based infrastructure. The system is internet based and requires secure login credentials to operate, enabling secure, unclassified usability by the warfighter.



Figure A-8. Windtalker

MOBILE-LOW, SLOW, SMALL UNMANNED AIRCRAFT INTEGRATED DEFEAT SYSTEM (M-LIDS)

A-15. The Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System (known as M-LIDS) is a C-UAS system that can detect, identify, track, and defeat UAS threats (see figure A-10 on page 76). It is mounted on two mine-resistant ambush protected vehicles for employment at the short halt. M-LIDS uses Forward Area Air Defense Command and Control system software and a mission data recorder connected via secure communications links. It includes one EW vehicle and one lethal defeat vehicle.

- EW vehicle—
 - Incorporates LIDS based configuration on a mobile platform.
 - Provides electronic detect, identify, track, and defeat capabilities.
 - Incorporates a .50 caliber machine gun for protection with an electro-optical infrared camera gun system (target acquisition range 2 kilometers).
- Kinetic defeat vehicle—
 - Provides detect, identify, track, and lethal defeat capabilities.
 - Incorporates the Coyote Block 2 interceptor; XM914, 30-caliber machine gun; and M240, 7.62-millimeter medium machine gun.
 - Mounts an electro-optical infrared camera gun system (target acquisition range 2 kilometers).
 - Includes KuRFS mobile radar that provides air surveillance and fire control at the short halt.
 - vehicle should remain within 50 meters of EW vehicle with an active CREW system
 - vehicle must be cleared of personnel and material to 150m at +/- 40 degrees at the boresight of the launcher to account for sabot ejection at time of launch.”

A-16. The Forward Area Air Defense Command and Control (FAAD C2) system provides engagement operations, aircraft avoidance, and fratricide prevention. As noted previously, the Forward Area Air Defense Command and Control system is interoperable with Link-16.



Figure A-10. Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System (M-LIDS)

HIGH ENERGY LASER

A-17. The high energy Laser (known as HEL) uses pure energy to detect, identify and defeat UAS threats (see figure A-11). HEL employs a multi-spectral targeting system that emits beams of light to defeat hostile UAS. The system is mounted on a Polaris MRZR all-terrain vehicle. The HEL has-

- Capability of targeting a single UAS with precision.
- Intuitive remote single user interface.
- Recharge capability for continuous operation.
- Ability to accept target cueing from existing surveillance, tracking radars.
- Modular architecture that can be integrated on multiple ground or airborne vehicles in palletized or podded configuration.



Figure A-11. High energy laser (HEL)

FIM-92 SHOULDER-FIRED, MAN-PORTABLE AIR DEFENSE SYSTEM

A-18. The FIM-92 man-portable air defense system (MANPADS) Stinger is an infrared homing shoulder-fired, portable surface-to-air missile (see figure A-12 on page 78). The missile can be deployed for defense against fixed- and rotary-wing aircraft, and UAS. The handheld launcher consists of a launch tube, battery coolant unit, separable gripstock assembly, sight assembly and separate IFF interrogator. The entire system weighs 35 pounds. The Stinger is operated by two operators and can be employed in all weather conditions. The MANPADS capabilities include-

- Fires basic and reprogrammable micro-processor block 1 missiles with no modification required.
- Gripstock:
 - Contains all pre-launch electronics and IFF antenna for MANPADS use.
 - Reusable for multiple firings.
- Battery coolant unit:
 - Contains thermal battery and argon gas coolant.
 - Expendable; supports one missile launch.
- IFF Interrogator:
 - Contains IFF system electronics and removable power source.
 - IFF compatible with U.S./NATO equipment.
- Integrated Forward Area Air Defense Command and Control system Software.

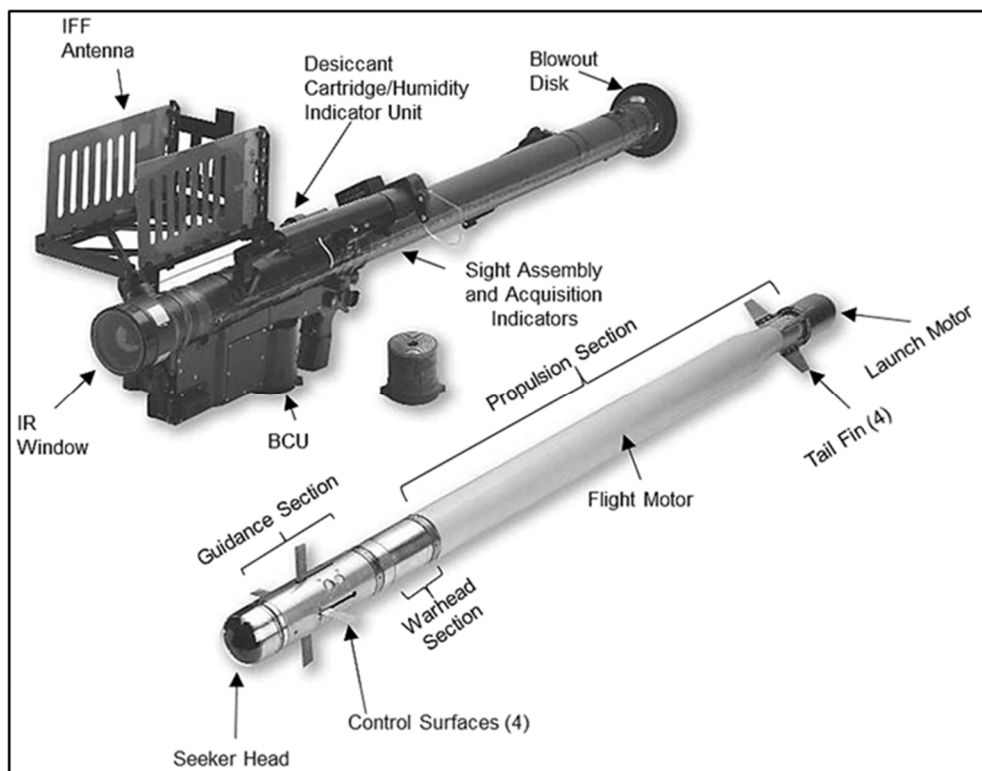


Figure A-12. Stinger FIM-92 man-portable air defense system

BAL CHATRI

The Bal Chatri is a passive RF detection capability used to detect and identify threat UAS (see figure A-13). The system employs a software defined radio RF detection system used to detect and identify enemy UAS. The radio can be configured for body-worn detection capability or for a small, fixed site location. Bal Chatri can also be integrated with a counter radio-controlled improvised explosive device electronic warfare system such as Modi. Limitations, system excludes automatic target detection and tracking source. Also, the operator must determine general directions of the target prior to system transmit.

A-19. System requires continual battery charging intervals to maintain system readiness. Bal Chatri Version 2 is a passive RF detection capability used to detect and identify enemy UAS. This system provides—

- Multi-band inter/intra team radio battery (up to 4 hours of battery life).
- Alternate power adapter provided.
- Universal serial bus and wireless networking capabilities.
- Built-in alerts.
- Improved light emitting diode visibility; night vision compatible.
- Ruggedized construction: meets defined test specifications for dust, water immersion, sand, vibration, and shock/drop.
- Flexibility to support multiple configurations and interface with multiple external systems for extended detect and defeat capabilities.
- Custom hardware includes dual simultaneous receive channels, high-speed detection scans (<5 seconds), and increased detection ranges.
- Spectral analysis and archiving tools.
- Also be integrated with counter radio-controlled improvised explosive device electronic warfare system such as MODI.

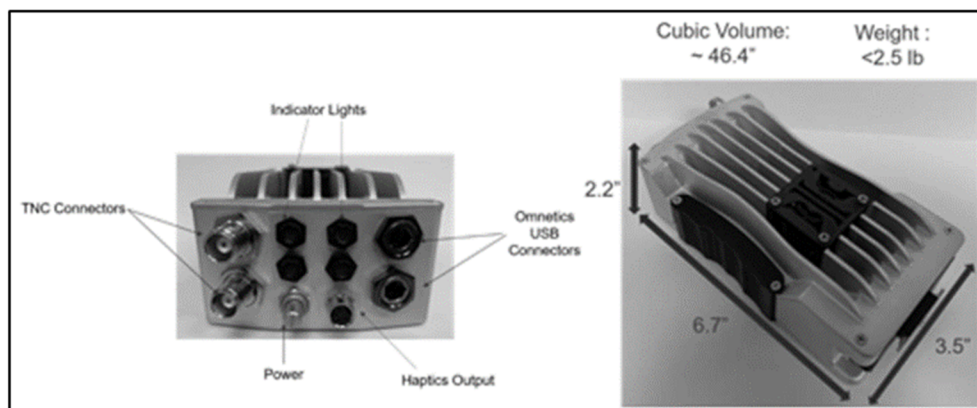


Figure A-13. Bal Chatri

DRONEBUSTER

A-20. The Dronebuster provides detect and defeat capability against threat UAS. It is a lightweight, handheld, battery operated, dismounted, EA device specifically designed to defeat UAS (see figure A-14 on page 80). The Dronebuster requires one person and is a standalone system. User interface is controlled via switches on the unit and a trigger. Light emitting diodes provide visual cues of the reporting status of the unit, its battery status, and the presence of a target enemy UAS downrange.

A-21. The unit exploits weaknesses in UAS communication protocols enabling the operator to jam the control signal forcing the unmanned aircraft to execute pre-programmed "lost signal" protocols. The system—

- Defends against groups 1 and 2 UAS.
- Operates strictly LOS.
- Requires the operator to keep "eyes on target" throughout engagement.
- If LOS to an engaged target is broken, control may still be regained.
- Designed to disrupt remote control (915 MHz, 2.4 GHz, and 5.8 GHz) and PNT guided UAS from approximately 400 meters.
- Jams UAS command and control and PNT links simultaneously, depending on system settings.
- May or may not have effects on target depending on UAS flight mode/capability.



Figure A-14. Dronebuster

SMART SHOOTER

A-22. The Smart Shooter enables the operator to defeat UAS threats. It is a rail mounted, smart electro-optic developed to enhance lethality of units engaged in C-UAS operations (see figure A-15). Smart Shooter is compatible with existing military rifles and can be mounted on any rail on a weapon system. When the Smart Shooter is employed it—

- Performs target lock, track and fire control capabilities.
- Provides a reliable push button targeting capability using an internal computer and image processor to deliver real-time firing solutions and a trigger interrupt feature (assisted firing).
- Can track and hit group 1 UAS up to 120 meters.
- Uses image processing to automatically acquire a target from the sight's field of view.
- Displays a box around the target in the shooter's reflex sight.
- Enables the shooter to select and lock on to the target.
- Will fire only when the sight is aligned to hit the target (includes required "lead" on a moving target).



Figure A-15. Smart shooter

MODI

A-23. The Modi is a dismounted, man portable EW system that enables detect and defeat capability (see figure A-16). Modi systems provide integrated tactical EW capabilities to defeat many UAS and other threats. The unit may be employed solely as a dismounted system or, using a mounted power amplifier, may be used in a fixed site or mounted configuration and dismounted when required. The Modi—

- Dismounted weighs 40.25 pounds (with pack).
- Operates at a wide temperature range (-20 to 60 degrees Celsius/-4 to 140 Fahrenheit).
- Can be integrated with multiple C-UAS and EW systems.



Figure A-16. Modi

FORWARD AREA AIR DEFENSE COMMAND AND CONTROL (FAAD C2)

A-24. FAAD C2 is a real-time safety critical C2 software application providing a single integrated air picture, airspace coordination and deconfliction, and fire control to support (see figure A-17 on page 82). This can be interconnected with the sheltered and handheld subsystems, the ADAM cell, Medusa (USAF), Avenger and various other FAAD C2 subsystems. Additionally, FAAD C2 software provides a three-dimensional (3D) view of objects displayed on the Battlefield Situation Display (BSD) of a visual representation of the flying aircraft and airspace control measures in the operator's area of responsibility.

A-25. Missions that FAAD C2 support including:

- Counter-Rocket, Artillery, Mortar Intercept Land-Phalanx Weapon System
- Maneuver-Short Range Air Defense (M-SHORAD)
- Low, Slow, Small, UAS, Integrated Defeat System (LIDS)
- Avenger

A-26. FAAD C2 uses the following communication systems:

- Link 16
- Link 11/11B
- Joint Range Extension Application Protocol
- Advanced Tactical Data Link
- Dedicated Fire Control Networks

A-27. FAAD C2 provides an air picture to engagement and force operations via government-owned interfaces and based on data gathered from various sensors. The FAAD C2 is integrated with over 25 sensors, including:

- AN/MPG-64 Sentinel
- AN/TPQ-50 Lightweight Counter Mortar Radar
- AN/TPQ-53 Counterfire Target Acquisition Radar
- Indirect fire protection capability
- High energy laser
- High power microwave
- Low, Slow, Small, UAS, Integrated Defeat System (LIDS)
- Ku-band Radio Frequency System Radar
- Lightweight Surveillance Tracking and Acquisition Radar
- Various EO/IR Systems.



Figure A-17. FAAD C2

RAJANT

A-28. RAJANT utilizes wireless networking to form a mesh network. The network is mobile, self-integrating, self-meshing, self-healing, and secure. The RAJANT provides flexibility, adaptability, and simplicity ensuring rapid deployment of a broadband wireless network into any situation. The network can be deployed as a stand-alone wireless network or bridged to another network (such as the Internet) utilizing available communication links such as a digital subscriber line, cable, or satellite modem. The RAJANT provides high bandwidth for applications to stream video, audio as well as data over large distances. The network traffic can be secured by using a selection of available security features. This makes the network optimal for tactical deployments and mission critical activities. Example of the RAJANT and components shown in figure A-18.

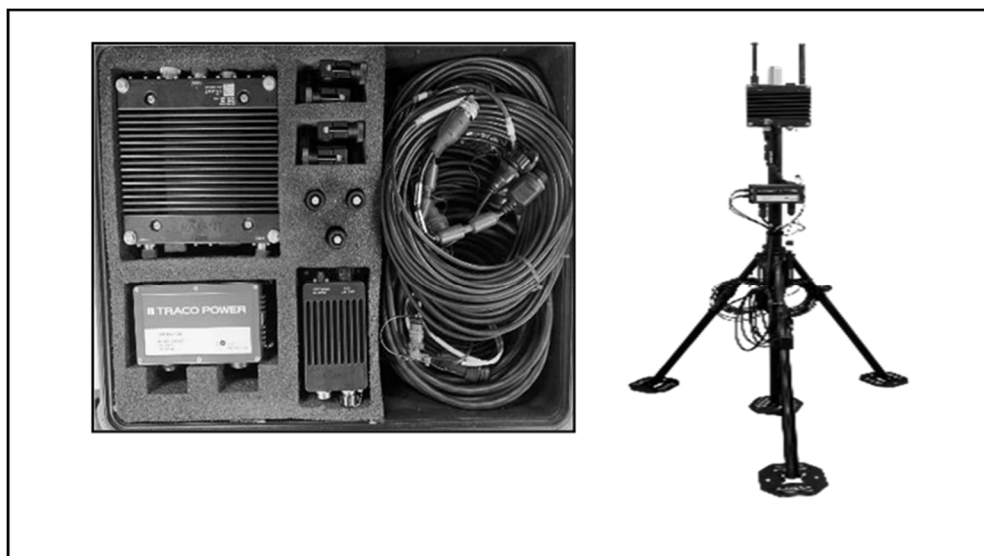


Figure A-18. Rajant

This page intentionally left blank.

Glossary

SECTION I – ACRONYMS AND ABBREVIATIONS

AADC	area air defense commander
ADA	air defense artillery
ADAM/BAE	air defense airspace management/brigade aviation element
ADW	air defense warning
AMD	air and missile defense
AO	area of operations
C2	command and control
CEMA	cyber electromagnetic activities
CORIAN	Counter-Remote Control Model Aircraft Integrated Air Defeat Network
C-RAM	counter-rocket, artillery, and mortar
C-UAS	counter-unmanned aircraft system
EA	electromagnetic attack
EME	electromagnetic environment
EMS	electromagnetic spectrum
EP	electromagnetic protection
EW	electromagnetic warfare
FAAD C2	Forward Area Air Defense Command and Control
FS-LIDS	Fixed Site-Low, Slow, Small Unmanned Integrated Defeat System
PNT	position, navigation, and timing
HEL	high energy laser
HN	host nation
IFF	identification, friend or foe
IPOE	intelligence preparation of the operational environment
ISR	intelligence, surveillance, and reconnaissance
KuRFS	Ku-Band Function Radio Frequency Sensor
LOS	line of sight
LPWS	Land-Based Phalanx Weapon System
L-MADIS	Light-Marine Air Defense Integrated System
MANPADS	man-portable air defense system
M-LIDS	Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System
NINJA	Negation of Improvised Non-State Aerial-Threat
OE	operational environment
ONS	operational needs statement
RF	radio frequency
ROE	rules of engagement
TTP	tactics, techniques, and procedures
UA	unmanned aircraft
UAS	unmanned aircraft system
VACR	visual aircraft recognition

SECTION II – TERMS

active defense

The employment of limited offensive action and counterattacks to deny a contested area or position to the enemy. See also passive defense. (JP 3-60)

cease engagement

A fire control order used to direct air defense units to stop tactical action against a specified target. (ATP 1-02.1)

electromagnetic attack

Division of electromagnetic warfare involving the use of electromagnetic energy, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. (JP 3-85)

electromagnetic interference

Any electromagnetic disturbance, induced intentionally or unintentionally, that interrupts, obstructs, or otherwise degrades or limits the effective performance of electromagnetic spectrum-dependent systems and electrical equipment. (JP 3-85)

electromagnetic protection

Division of electromagnetic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy use of the electromagnetic spectrum that degrade, neutralize, or destroy friendly combat capability. (JP 3-85)

electromagnetic support

Division of electromagnetic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. (JP 3-85)

electromagnetic warfare

Military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. (JP 3-85)

engage

In air and missile defense, a fire control order used to direct or authorize units and/or weapon systems to attack a designated target. (JP 3-01)

hold fire

An emergency fire control order to stop firing on a designated target and destroy missiles in flight. (ATP 1.02.1)

operational environment

The aggregate of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. (JP 3-0)

passive defense

Measures taken to reduce the probability of and to minimize the effects of damage caused by hostile action without the intention of taking the initiative. See also active defense. (JP 3-60)

risk management

The process to identify, assess, and mitigate risks and make decisions that balance risk cost with mission benefits. (JP 3-0)

rules of engagement

Directives issued by competent military authority that delineate the circumstances and limitations under which United States forces will initiate and/or continue combat engagement with other forces encountered. (JP 3-84)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (ADP 5-0)

unmanned aircraft system

That system whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. (JP 3-30)

weapons control status

An air and missile defense control measure declared for a particular area and time by an area air defense commander, or delegated subordinate commander, based on the rules of engagement that establish the conditions under which fighters and surface air defense weapons are permitted to engage threats. (JP 3-01)

weapons free

Weapons free is the least restrictive status: used to indicate when any target not positively identified as friendly in accordance with current ROE may be engaged. (JP 3-01)

weapons hold

Weapons hold is the most restrictive status. Units may only fire in self-defense or when ordered by proper higher authority. (JP 3-01)

weapons tight

Weapons tight is the normal status. Units may only fire on targets identified as hostile in accordance with current ROE. (JP 3-01)

This page intentionally left blank.

References

All websites accessed 09 May 2025.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

Army Dictionary available at <https://jdeis.js.mil/jdeis/index.jsp?pindex=207>.

DOD Dictionary of Military and Associated Terms. 15 February 2025.

FM 1-02.1. *Operational Terms*. 28 February 2024.

FM 1-02.2. *Military Symbols*. 23 January 2025.

RELATED PUBLICATIONS

These documents are cited in the publication.

JOINT PUBLICATIONS

Unless otherwise indicated, most joint publications are available online at <https://www.jcs.mil/Doctrine>.

JP 3-0. *Joint Campaigns and Operations*. 18 June 2022.

JP 3-01. *Countering Air and Missile Threats*. 06 April 2023.

JP 3-30. *Joint Air Operations*. 25 July 2019.

JP 3-60. *Joint Targeting*. 20 September 2024.

JP 3-84. *Legal Support*. 02 August 2016.

JP 3-85. *Joint Electromagnetic Spectrum Operations*. 22 May 2020.

ARMY PUBLICATIONS

Most Army publications are available online at <https://armypubs.army.mil/>.

ADP 3-0. *Operations*. 21 March 2025.

ADP 5-0. *The Operations Process*. 31 July 2019.

AR 11-33. *Army Lessons Learned Program*. 28 July 2022.

AR 71-9. *Warfighting Capabilities Determination*. 29 June 2021.

ATP 1-02.1/MCRP 3-30B.1/NTTP 6-02.1/AFTTP 3-2.5/STTP 3-9002. *Multi-Service Tactics, Techniques, and Procedures for Multi-Service Brevity Codes*. 25 April 2025.

ATP 3-01.8. *Techniques for Combined Arms for Air Defense*. 29 July 2016.

ATP 3-12.3. *Electromagnetic Warfare Techniques*. 30 January 2023.

ATP 5-19. *Risk Management*. 09 November 2021.

ATP 6-02.70. *Techniques for Spectrum Management Operations*. 16 October 2019.

FM 3-0. *Operations*. 21 March 2025.

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

FM 6-27/MCTP 11-10C. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.

FM 7-0. *Training*. 14 June 2021.

TC 3-01.80. *Visual Aircraft Recognition*. 5 May 2017.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website:
<https://armypubs.army.mil/>.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

RCOMMENDED READINGS

These documents contain relevant supplemental information.

ATP 3-01.16. *Air and Missile Defense Intelligence Preparation for the Battlefield*. 31 March 2016.

ATP 3-01.60. *Counter-Rocket, Artillery, and Mortar Operations*. 10 May 2013.

Counter-Small Unmanned Aircraft Systems Home Station Training Support Package & Administrative Guide. 03 May 2023. <https://atn.army.mil/getmedia/72734f47-9d87-4ffa-b672-afb71fbd520a/CUAS-HS-TSP-Administrative-Guide-c1-20230503-FINAL.pdf>.

(Common access card [CAC] login required. Refresh page after login.)

FM 3-13. *Information Operations*. 06 December 2016.

Index

Entries are by paragraph number.

A

ADAM/BAE, 2-10, 4-19, 5-3, 7-25
air and missile defense, 2-15, AMD, 6-1, 6-2, 6-4, 6-8, 6-16, 6-17, 6-19, 6-22,
air defense airspace management, 2-10
air defense warning, 85
area air defense commander, 6-2, AADC, 6-2, 6-5, 6-13, 6-18
area of operations, 1-2, 4-36, 4-42, 5-5, 6-1, 6-14

B

brigade aviation element, 2-10

C

command and control, 1-6, 3-2, 3-5, 4-17, A-2, A-8, A-9, A-15, A-16, A-18, A-21, A-24

cyber electromagnetic activities, 2-12, CEMA, 2-6, 2-7, 2-12 to 2-14, 4-24, 7-25

E

electromagnetic attack, 2-7, 3-2, 4-24
electromagnetic environment, 4-36, EME, 4-36, 4-42,
electromagnetic protection, 4-25
electromagnetic spectrum, 2-17, 4-23, 4-25, 4-27
electromagnetic warfare, 1-6, 2-6, 2-7, 2-12, 2-13, 3-2, 4-23 to 4-26, 5-20, A-2,

H

host nation, 4-12

I

identification, friend or foe, A-13
intelligence preparation of the operational environment, 4-9

intelligence, surveillance, and reconnaissance, 1-6, 3-2

O

operational environment, 1-1, 4-9
operational needs statement, 7-5

P

position, navigation, and timing, 1-4, 1-13, A-1, A-2

R

radio frequency, 4-36, 5-26, 5-33, A-5, A-7, A-27
rules of engagement, 2-10, 2-11, 2-17, 6-6

T

tactics, techniques, and procedures, 4-14m TTP, 4-14, 4-36, 5-4, 5-8, 7-10, 7-14, 7-15, 7-19, 7-22, 7-28, 7-29, 7-30 to 7-32

This page intentionally left blank.

ATP 3-01.81

23 May 2025

By Order of the Secretary of the Army:

RANDY A. GEORGE

*General, United States Army
Chief of Staff*

Official:

A handwritten signature in black ink, appearing to read 'Mark F. Averill', written in a cursive style.

MARK F. AVERILL

*Administrative Assistant
to the Secretary of the Army
2514204*

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve. Distributed in electronic media only(EMO).

This page intentionally left blank.

This page intentionally left blank.

