United States Army
Counter - Unmanned Aircraft System (C-UAS)
Strategy Extract

October 5, 2016

Distribution A. Approved for public release: distribution unlimited

C-UAS Strategy Framework

"Meeting the UAS challenge"

Ways (How)

Employ three broad actions to direct the allocation of future efforts and resources:

- Pursue Joint Combined Arms Solutions
- Integrate capabilities across all domains
- Adopt a whole-of-government approach

Linkages

- Joint Integrated Air and Missile Defense Vision and Roadmap
- Army Operating Concept
- Army Warfighting Challenges
- Army AMD Strategy

Means (What)

Examine Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Policy (DOTMLPF-P) endeavors, organized by and across the Lines of Effort, to ensure capability to respond to current and emerging UAS threats

DOTMLPF-P	Lines of Effort
Doctrine	**LOE 1: Mission Command** • Airspace Control and Airspace Management • Rules of Engagement and Risk Management • Tactical Air Picture and Early Warning
Organization	
Training	**LOE 2: Detection** • Radar Improvements • Electro-optic & Infrared Sensors • Acoustic Sensors • Visual & Audible • Other Sensors
Materiel	
Leader Development	**LOE 3: Identification** • Electronic • Procedural • Visual
Personnel	
Facilities	**LOE 4: Defeat (Kinetic & Non-Kinetic)** • Left of Launch • Standoff Engagements • Close Contact Engagements
Policy	

Ends (Outcome)

The Army develops and provides a comprehensive set of capabilities that enable current and future commanders at all echelons to detect, identify, and defeat threat UAS.

Priorities

Near

Repurpose and adapt current programs, systems, and formations to include updates to doctrine and training

Mid-Far

Develop new capabilities to enhance the combined armed approach focusing on adversaries' changes in systems and tactics

Table of Contents

CHAPTER 1. Introduction

1-1. Purpose

This strategy is the Army's effort to integrate and synchronize C-UAS efforts across the Army, and to inform joint, inter-organizational, and multinational (JIM) partners about the Army C-UAS efforts. This strategy frames the C-UAS mission set, presents the ends, ways, and means, and prescribes C-UAS lines of effort in an unified approach to defeat threat UAS.

1-2. Background

a. Analysis of the future operational environment and recent military operations around the globe, clearly illustrates the seriousness of the UAS threat. The Army C-UAS capabilities, past, current and future cross every warfighting function and many JIM partners capabilities play a role in defeating all threat UAS. This strategy represents the effort to align C-UAS efforts across the force.

b. The strategy will address focus on Groups 1-3 UAS since they pose challenges to the force that are less effectively countered by existing integrated air and missile defense (IAMD) capabilities. Smaller sized UAS, Group 1-3, are more challenging targets to consistently defeat due to their ease of proliferation and low/slow kinematic profile, especially in congested airspace with standoff surveillance capabilities and limited detection/engagement windows.

c. This strategy seeks to provide forces at all echelons with solutions across the doctrine, organization, training, material, leadership, personnel, facility-policy (DOTMLPF-P) framework that will enable defeat of UAS threats. It seeks *combined arms solution*s, utilizing capabilities from every warfighting function, in a coordinated, synchronized way. It seeks *cross-domain solutions*, recognizing that the C-UAS mission set exists in every domain, not just in the air. Finally, it seeks a *whole-of-government approach*, recognizing that a comprehensive C-UAS capability will involve JIM partners from all areas of government, working together towards a common goal.

1-3. Assumptions

All assumptions from the Army Capstone Concept (ACC) and the Army Operating Concept (AOC) apply to this strategy. In addition, the following assumptions have been identified:

- UAS will become smaller, cheaper, and more capable as technology evolves.
- UAS proliferation will increase as UAS become more capable and less expensive.
- Related new technologies will emerge/evolve that enhance UAS operations.
- Future decisions will provide adequate resources and organizational structure to support C-UAS capabilities development.
- Current and future IAMD capabilities, to include surface-to-air systems, air-to-air systems, Command and Control Systems, are adequate to deal with large UAS.
- The cyber domain and electromagnetic spectrum will be more contested in the future. Adversaries will challenge the United States in these areas due to evolving technology and proliferation.
- Army and JIM partners will continue development of integrated cooperative identification technologies for application onto most or all friendly UAS platforms.

1-4. The Army C-UAS Strategy accounted for and provides linkage to:
- The Joint Integrated Air and Missile Defense: Vision 2020 (2012) and the Roadmap for Joint Integrated Air and Missile Defense (JIAMD) 2020-2030 (2014).
- The Army Operating Concept (AOC) and the Army Warfighting Challenges (AWFCs)

CHAPTER 2. Operational Environment

2-1. Background.
Unmanned Aircraft Systems (UAS) have advanced technologically and proliferated exponentially over the past decade. As technology has progressed, both reconnaissance and attack capabilities have matured to the point where UAS represent a significant threat to Army operations from both state and non-state actors.

2-2. UAS Threat Types and Observations.
"Groups" are the most widely used and recognized means to classify UAS. The numerical definitions use performance characteristics:

- Group 4 and 5 UAS are known to fly high and have long distance platforms. They tend to operate at speeds and altitudes and are similar in size to manned aircraft, performing missions that are operational or strategic in nature.

- Smaller UAS platforms, Groups 1-3, are slower and have shorter-range than the larger UAS. As UAS have become smaller, slower and operate at lower altitudes, they have become more challenging to detect, identify, and defeat. Technological advances have exacerbated these challenges. These systems can be either proprietary, state sponsored or commercial-off-the-shelf (COTS). Typical roles for these UAS are limited-scale reconnaissance and surveillance. However, miniaturization of components will make these UAS more capable in the future. This, coupled with their small size, low cost, and widespread availability will drastically increase their use worldwide.

2-3. Proliferation.
a. Currently, there are more than 600 types of UAS used in over 80 countries. Most countries that domestically produce UAS have either the same or like models available for sale to foreign governments. The production of small UAS is simple, rapid, and inexpensive. Estimates vary from 80,000 to half a million drones now operating in U.S. airspace, and the Consumer Electronics Association estimates that 700,000 new UAS will be sold to commercial and recreational users in the U.S. this year alone.

b. The proliferation of UAS has created an airspace environment in which target identification is an issue. Many countries now deploy the same or similar models of UAS leading to issues with combat identification; similarly, users often combine components from different manufacturers to create ad-hoc "hybrid" UAS. Distinguishing friendly from other UAS may be possible through technical means, but difficulties from proliferation of similar systems is systemic and unlikely to decline in the near- to mid-term.

2-4. Vignette - from a collection of open-source reporting

With skies contested by large numbers of highly lethal counter-air systems and a pressing need for full spectrum ISR, Moscow and Kiev both have deployed large numbers of UAS in support of their operations in the Crimea. Both sides are using unarmed reconnaissance drones to inform their forces about the opponent's movements and positions. One UAS capability in particular has emerged as a substantial enabler: target acquisition for artillery. One analyst has described the UAS targeting of the Russian-backed separatists as the most significant difference-maker in a conflict between otherwise equal forces. Ukraine's military has not invested heavily in UAS capabilities; as a result, Ukraine's forces have resorted to improvising new homemade drones and buying whatever they can from allies and the commercial market. In contrast, Russian-backed rebels in Ukraine have access to cutting edge UAS technology. Moscow has supplied these rebels with both indigenous Russian and foreign systems, including from Israel, France, and China. In addition, the rebel's electronic warfare systems far exceed that of Ukraine, allowing the rebels to control the electromagnetic spectrum and effectively neutralize Ukrainian UAS while allowing their own freedom of maneuver.

The current Russian advantage in UAS capability stems largely from lessons learned in a past conflict: Russia's 2008 war with Georgia. Though the Russians easily defeated Georgia's tiny military, Georgian forces made extensive use of Israeli-made UAS in ISR roles, illustrating their potential to Russian forces. Soon after, the Russians implemented a massive UAS development program, buying large numbers of Israeli UAS and investing billions in domestic UAS programs. Despite their late start, Russia's UAS program paid dividends in Ukraine. A U.S. Army spokesman, said in a recent interview, that Russian drones are a major contributing factor to the rebel's extraordinarily accurate artillery.

Russian drones confirmed to be operating in the Crimea include the Orlan-10, the Granat-1, and the Takhion. All of these drones are tactical: they are physically small and fly low, slow profiles. All have modular ISR packages and all are used in conjunction with artillery units to increase accuracy in the target location and response in counterfire. Separatist forces claim that the Granat-1 doubles the accuracy of artillery battalions equipped with them. Typically, rebel forces are equipping artillery battalions with tactical UAS, usually at the target acquisition platoon. Russian tactical UAS can be moved into position and launched very quickly (< 20 minutes), allowing artillery battalions to utilize these systems in support of rapidly moving maneuver units. The systems utilize modular sensor suites allowing commanders to tailor the sensor to the mission and conditions; optical sensor s for good weather, IR or electronic surveillance for bade weather, audio and flash sensors for counterfire missions. These UAS digitally pass accurate target location data to their operators, who are closely integrated with shooters. Minimal restrictions allow shooters to engage and destroy targets rapidly, even when targets are concealed or hardened. Most of these UAS do not need to overfly hostile territory and conduct their ISR from standoff distances.

CHAPTER 3. Meeting the UAS Challenge: Ends, Ways and Means.

3-1.Ends. The Army develops and provides a comprehensive set of capabilities that enable current and future commanders at all echelons to detect, identify, and defeat threat UAS and enjoy strategic and tactical freedom of maneuver and action through all domains including the electromagnetic spectrum (EMS): home and abroad.

3-2. **Ways.** There is no single, comprehensive materiel solution that will make the UAS problem disappear; nor does a single Army, joint, or multinational capability that can, from either a proficiency or sufficiency standpoint, defeat the UAS threat. Success in the C-UAS mission requires integration of numerous capabilities that stretch across all seven warfighting functions and across all twenty Army Warfighting Challenges. This strategy proposes three broad actions to direct the allocation of future efforts and resources: pursue Joint Combined Arms Solutions, integrate capabilities across all domains, and adopt a whole-of-government approach.

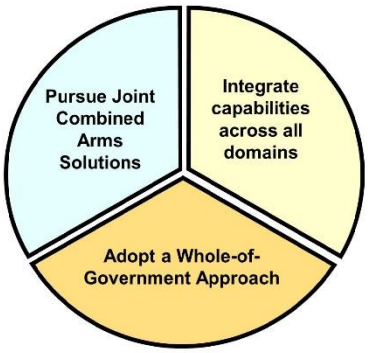

Figure 1: "Ways"

a. *Pursue Joint Combined Arms Solutions*. Joint combined arms operations seek to synchronize capabilities in such a way that achieve mutually complementary effects; including both traditional military combat systems and the broad range of JIM capabilities necessary to accomplish a given mission. The C-UAS mission must be viewed as an inherently combined arms operation despite being seen as an Air Defense only problem; one which Army, joint, and multinational air defense forces must address unilaterally. While air defense forces play a key role in C-UAS, Army, joint and multinational air defense formations are insufficient in both quantity and capability to address the threat alone. In the JIM realm, Fires forces integrate surveillance capabilities, identify targets, and facilitate and conduct engagements. Protection and intelligence forces integrate cover, concealment, and deception (CCD) and situational awareness capabilities. Electronic Warfare and other Cyber Electro-Magnetic Activity (CEMA) type cells exploit and integrate cyberspace operations, Electronic Attack (EA) and Electronic Protection (EP) capabilities. Maneuver forces contribute to surveillance and identification while conducting engagements of threat systems. Mission Command integrates capabilities, implements plans, enhances situational awareness and understanding, and enables leaders' decision-making. The goal of this solution seeks an endstate where a rapid and seamless integration of capabilities aggressively addresses the entire spectrum of the UAS threat, from the national strategic level down to the individual Soldier. Once operations commence, the objective is to disrupt threat UAS operations "left-of-launch" both kinetically (strike) and non-kinetically (CEMA or EW/Cyber) using both passive and active measures seek to defeat systems before their effects can be employed.

b. *Integrate capabilities across all domains.* Joint combined arms is, by definition, multi-domain. This strategy emphasizes the role of integrating capabilities that cut across multiple domains, illustrating the joint combined arms approach necessary for a successful C-UAS

capability. On land, Army and JIM forces target UAS ground stations and support facilities utilizing integrated air, space, ground, and EMS sensors to accurately locate targets. Ground stations and support facilities are disrupted or destroyed through synchronized and integrated fires including EA. At sea, Army forces integrate with JIM partners to detect, identify, and engage threat UAS operating over water. In the air, UAS are detected, identified, and defeated by a variety of kinetic and non-kinetic means. This includes air defense, direct fire and EW, along with CCD efforts. In space, advanced threat UAS that integrate space-based capabilities are disrupted through space control measures where space-based sensors contribute surveillance and targeting data to Army and JIM systems enabling defeat efforts in other domains. In cyberspace, Army and JIM cyber capabilities are employed to surveil, disrupt, degrade, or destroy threat UAS. Threat networks to include UAS control systems are attacked, tactical commanders are enabled via a cyber-common operating picture (CCOP).

c. *Adopt a Whole-of-Government Approach*. The Army Operating Concept extends Joint Combined Arms to encompass enablers and capabilities from across all Army and JIM organizations and cooperate with JIM partners in developing and implementing a comprehensive C-UAS strategy. Multinational partners have already begun implementing aggressive C-UAS plans of their own, and by combining efforts and sharing knowledge, US forces can maximize the effects of limited resources; however, joint efforts must be coordinated and synchronized with JIM efforts to avoid redundancies and conflicts. Multinational partners will, as always, be important participants in the C-UAS fight. Strategic considerations (basing, sustainment, etc.) will set the stage for a successful C-UAS mission. These require building partner capacity long before hostilities commence. Inter-organizational partners play a prominent role in the C-UAS mission set and efforts between the Army and inter-organizational partners must be coordinated and synchronized in much the same way as the joint services.

3-3. Means. There are four Lines of Effort (LoEs): Mission Command, Detection, Identification, and Defeat. This aligns with the problems identified in the 2012 and 2014 C-UAS CONOPS. Select lines of effort are bifurcated into two distinct areas: near-term, and mid/far-term. Near-term is intended to cover the timeline through the year 2020; mid- and far-term looks at five to 25 years from the present time. These lines of effort are intended as broad discussions of capabilities.

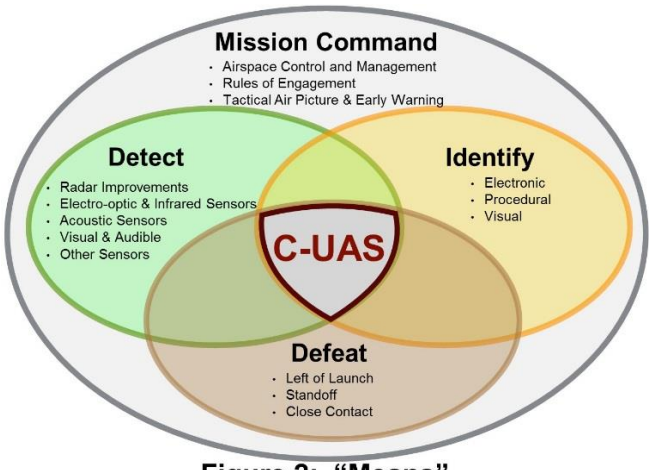

Figure 2: "Means"

a. Mission Command. Underpinning the "detect, identify and defeat" methodology is the ability to effectively understand, integrate, and command those capabilities.

(1) Airspace Control and Management. Effective airspace management is a cornerstone to any successful counter-air operation to including supporting and controlling manned/unmanned aircraft, clearing and authorizing fires through airspace, and supporting positive and procedural identification of targets of all types. In the long-term, the Army must pursue automated dynamic airspace management tools that will provide instantaneous clearance and dynamic airspace control to commanders.

(2) Rules of Engagement (ROE) and Risk Management. Having ROE that are properly tailored to the situation will facilitate timely engagements of threat systems while mitigating the chances of fratricide.

(3) Tactical Air Picture and Early Warning. Commanders need to provide their subordinates with UAS early warning when possible. All C-UAS measures are more effective when systems and operators have advanced notice, and a higher quality and quantity of the warning enables more effective C-UAS measures. In the near term, commanders will utilize existing Army and joint data networks to promulgate data to the lowest possible echelon; long term will require a comprehensive, tailorable Common Operating Picture (COP) distributed automatically to all Soldiers who require it.

b. Detection. This line of effort examines and integrates the multiple programs and initiatives that contribute to detecting UAS; promulgating that information to the affected commands. The size, composition, and flight profiles of theater and strategic UAS are equal in difficulty for detecting, tracking, and identifying as manned aircraft. However, other UAS typically have smaller radar cross sections, smaller IR signatures, and limited electromagnetic footprints. Current and future sensors require more advanced capabilities to effectively increase UAS detection. The five subordinate lines of effort for this task are: radar, other electromagnetic and electronic sensors, OE/IR, acoustic sensors, and visual/audible detection.

(1) Radar. Formations across the battlefield must have access to high quality radar data to inform commanders and support C-UAS operations. In the far-term, multi-mission sensors provide comprehensive radar detection and enhanced identification with fewer sensors.

(2) EO/IR sensors. Electro-optic and infrared (EO/IR) sensors can provide a search, detect, and track capability for all UASs. They can also provide resolved imagery which can be used for recognition and identification, either by human operator or an automated/aided system.

(3) Other Electromagnetic and Electronic Sensors. In addition to radars, formations must have the capability to detect UAS using other means. Being able to detect, and ideally locate the source, is an enabler to defeating the UAS threat set. In the near-term, emerging Electromagnetic and Electronic Sensor capabilities will contribute to this effort.

(4)Acoustic sensors. Acoustic sensors can be standalone or combined with other sensor modes for a fused sensor system providing a robust capability and a low false-alarm rate.

(5) Visual and Audible. For very small UAS, it is plausible that the first indication of their presence will be visually seeing or hearing the UAS due to their limited altitudes and ranges. Capabilities that allow for these non-electronic detections to be integrated into the joint tactical picture will enable early warning, commander decision-making, and defeat. Individual Soldiers must be trained to recognize the sound of a UAS, trained on visual scanning techniques, and be prepared to communicate critical target information (distance, direction, and type) to higher echelons.

c. Identification. Forces that have detected a UAS target now must identify its character: threat, friendly, or neutral. Upon detection, by any method, there remains a requirement to differentiate threat from friendly or neutral UAS to enable tactical and timely decision-making.

(1) Electronic. Electronic means of identification are typically the most sure and also the fastest, though they require the most resources. Improving friendly force identification tools, will allow the joint force to integrate reliable electronic identification capabilities on all aerial platforms, simplifying identification procedures at all levels. Emerging sensors that have the capability to identify targets based on radar cross section, IR signatures, or other electronic signatures should be integrated into identification processes. These capabilities greatly lessen the risk to friendly aircraft and thus allow commanders to implement a more aggressive ROE.

(2) Procedural. Procedural ID methods involve identifying a target based on behavior relative to established airspace control measures, point of origin, or other behavioral characteristics. Establishing airspace control measures at all echelons, including tactical, is a major enabler of this method of identification.

(3) Visual. Visual aircraft recognition is a key ID enabler for UAS defeat. While the number of UAS types is enormous and varied, they take on only a few primary physical forms. Training Soldiers to identify UAS based on a handful of primary characteristics (rotary-wing vs fixed wing, pusher vs tractor, etc) can give added information to assist in the hostile or friendly nature of target.

d. Defeat. The UAS threat requires a fully integrated combined arms approach. This strategy proposes a "defense-in-depth" methodology, wherein UAS operations are aggressively addressed through three distinct tiers: left-of-launch, standoff, and close contact. These tiers can be thought of as most preferential to least: ideally, UAS are defeated prior to launch, if not, then at standoff distances, then, if required, in close contact. Capabilities assigned to these tiers are not intended to be conclusive; rather, it is intended as a broad framework for providing defense-in-depth. Each of these capabilities are an option available to a commander to defeat UAS.

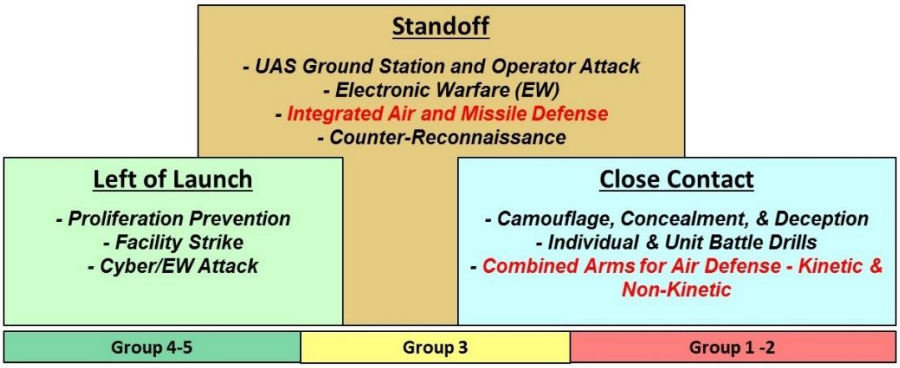

Figure 3: Defeat – "Defense in Depth"

(1) Left-of-Launch. Left-of-launch efforts attempt to defeat or disrupt UAS threats prior to their aerial vehicles ever being deployed. They are conducted across all levels of war. They will typically involve higher tactical and operational echelons in targeting and integrating electronic warfare and cyber capabilities, with synchronized diplomatic/political efforts.

a. Proliferation Prevention. As with many other potential threats, the United States and her allies must attempt to control the proliferation of UAS technology to threat nations and non-state actors as the diplomatic and political environment allows. While the simplicity and low cost of UAS technology makes it far more difficult to control than, some levels of interference are possible. The Army must interface with these branches of government assigned to this task and support their efforts.

b. Facility Strike. Attacking launch, maintenance, and command and control facilities is a method in counter-air campaigns. While not all UAS will have large and/or visible facilities, those that can be targeted must be a priority target for Army and joint planners. These actions will likely take place at higher echelons will be integrated through the targeting process. While this line of effort is identified as a left-of-launch initiative, in practice it must occur throughout operations.

c. Cyberspace and Electronic Warfare Operations. Many commercial and some military UAS are dependent on cyberspace and EMS capabilities for planning, command, and control. These capabilities must be targeted and attacked in the same way as are tangible facilities. These efforts are likewise integrated through targeting and must involve joint and multinational partners.

(2) Standoff. Standoff engagements seek to defeat or disrupt UAS operations prior to the employment of the UAS's capabilities. These options involve using offensive and defensive capabilities at longer ranges to deny the use of wide areas to threat UAS. Broadly speaking these capabilities will be employed at operational and higher tactical echelons, though some (particularly EW) will likely make their way to very low tactical echelons as new systems are fielded.

a. UAS Ground Station and Operator Attack. While related to the kinetic attack operations option above, this effort refers primarily to defeating deployed UAS through attacking ground stations and operators using joint-combined arms approach.

b. Electronic Warfare. The overall goal of Offensive Electronic Attack (OEA) involves the use of Electromagnetic (EM) energy and directed energy to control the Electromagnetic Spectrum (EMS) or to attack the enemy. EW efforts are integrated through targeting and will occur at all echelons as applicable and must be synchronized. All EW efforts require effective spectrum management operations to eliminate spectrum fratricide and protect friendly UAS operations.

c. Integrated Air and Missile Defense (IAMD). IAMD plays a key role in C-UAS at all echelons. Commanders and air defense planners must account for the UAS threat when establishing critical/defended asset lists, planning system deployments, and developing ROE. IAMD systems also play a key role in promulgating the joint tactical air picture across the force, especially to tactical echelons. Air Defenders within tactical formations must inform their commanders about threat UAS activities and then work to develop a defeat strategy that integrates all available capabilities.

d. Counter-Reconnaissance. Counter-reconnaissance seeks to undermine the threat's ability to conduct reconnaissance and surveillance efforts. UAS plays a significant role in reconnaissance for both threat and friendly forces; thus, all counter-reconnaissance plans must account for UAS.

(3) Close Contact. If both left-of-launch and standoff efforts fail to defeat or disrupt UAS operations, the task of defeating the UAS will likely fall on the unit or asset that the UAS is attacking or surveilling. These lines of effort can be thought of as a "last line of defense". Some threat UAS will be difficult to defeat left-of-launch or at standoff ranges. These lines of effort will be focused largely on the individual and small unit levels.

a. Individual and Unit Common Task Training. UAS are similar to previous broadly employed threat capabilities (artillery, air attack, IEDs, etc) that the Army has faced. When a particular threat capability can affect the entire force, individual and unit task training as a means to counter that threat becomes very important. UAS events must be treated as battle drills or "warrior tasks" by Soldiers and units: proper responses (reporting, engaging, finding cover) must be standardized and trained in both institutional and unit environments. Facilities must also be upgraded, enabling commanders and institutional training alike to conduct C-UAS as integral parts of training.

b. Camouflage, Concealment, Deception (CCD) and Hardening. The majority of UAS employed today and in the near future will not have an organic attack capability. Instead, they are used to detect and identify targets for other weapons systems, such as artillery. These systems can be defeated simply by eliminating their ability to detect their targets. Commanders at all echelons must emphasize CCD/hardening resourcing and training. Relatively simple solutions such as camouflage and smoke, can have a significant impact on threat UAS operations with minimal effort required by friendly forces. Hardening can defeat both attack UAS and fires enabled by UAS surveillance.

c. Combined Arms for Air Defense (CAFAD) and Other Direct Fire Engagements. When units are threatened by UAS operating outside the scope or capability of other defeat mechanisms, CAFAD engagements must be an option. CAFAD is broadly defined as the use of a unit's organic direct fire systems (including both kinetic and non-kinetic systems) to engage an aerial target. Commanders must assess the risk to their formation posed by threat UAS, the capabilities of their organic direct fire systems, and other available defeat mechanisms prior to making the decision to engage a target. Commanders must identify the target (and engage per their ROE), and must clear their fire both through the air and on the "beaten zone" (the area where rounds may fall).

CHAPTER 4. Governance Process

The Fires Center of Excellence (CoE), the Army lead for C-UAS, in coordination with other CoEs, leads an ARCIC directed Integrated Capability Development Team (ICDT) with a quarterly General Officer Steering Committee (GOSC). This synchronizes capability development and shares situational understanding about C-UAS gaps across the Army. Long-term equities are addressed in near-term approaches/agreements; existing developmental requirements and programs are informed about C-UAS developments. In addition, the Fires CoE, in cooperation with Army and JIM partners, develops recommended solutions and injects into the TRADOC, HQDA and other Joint governance processes.

CHAPTER 5. Conclusion

The Army's existing capabilities and ongoing work to counter threat UAS must be energized in conjunction with efforts that facilitate an Army-wide assessment across the domains. The Army recognizes this is not a one size fits all approach to the categorization of threat UAS nor to core tasks associated with C-UAS: detect, identify and defeat. Exploring interoperable and interdependent joint solutions and bridging some level of shared capability with our allied/partner nations, this strategy provides a relevant framework for incorporating immediate and interim measures to protect the force now, and provides the direction toward re-instituting a joint combined arms approach training strategy for offensive and defense C-UAS capabilities.