

NOVEMBER 2023



Countering Small Uncrewed Aerial Systems

Air Defense by and for the Joint Force

AUTHORS

Shaan Shaikh

Tom Karako

Michelle McLoughlin

A Report of the CSIS Missile Defense Project

CSIS

CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

NOVEMBER 2023

Countering Small Uncrewed Aerial Systems

Air Defense by and for the Joint Force

AUTHORS

Shaan Shaikh

Tom Karako

Michelle McLoughlin

A Report of the CSIS Missile Defense Project

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Thomas J. Pritzker was named chairman of the CSIS Board of Trustees in 2015, succeeding former U.S. senator Sam Nunn (D-GA). Founded in 1962, CSIS is led by John J. Hamre, who has served as president and chief executive officer since 2000.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—nonpartisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

CSIS scholars bring their policy expertise, judgment, and robust networks to their research, analysis, and recommendations. We organize conferences, publish, lecture, and make media appearances that aim to increase the knowledge, awareness, and salience of policy issues with relevant stakeholders and the interested public.

CSIS has impact when our research helps to inform the decisionmaking of key policymakers and the thinking of key influencers. We work toward a vision of a safer and more prosperous world.

CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

© 2023 by the Center for Strategic and International Studies. All rights reserved.

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Acknowledgments

The authors would like to thank all our peer reviewers who were so generous with their time and expertise, including Arch Macy, Peppi DeBiaso, Richard Formica, Francis Mahon, Jaron Wharton, and numerous others who provided critical feedback. We also wish to thank our colleagues Patrycja Bazylczyk, Masao Dahlgren, Wes Rumbaugh, and Ian Williams for their support in editing and producing this report.

This report was supported by Raytheon, an RTX business, and Epirus, Inc., as well as by general support to CSIS.

Abbreviations

ADA - Air Defense Artillery

AGL - Above ground level

AI/ML - Artificial intelligence and machine learning

APKWS - Advanced Precision Kill Weapons System

ATP - Army Techniques Publication

BLOS - Beyond line of sight

C2 - Command and control

CAFAD - Combined arms for air defense

CENTCOM - U.S. Central Command

CLWS - Compact Laser Weapons System

C-RAM - Counter-Rocket, Artillery, Mortar

C-sUAS - Counter-small uncrewed aerial systems

DE - Directed energy

DJI - Da-Jiang Innovations

DoD - Department of Defense

DOTMLPF - Doctrine, organization, training, materiel, leadership and education, personnel, and facilities

EO - Electro-optical

EW - Electronic warfare

FAAD C2 - Forward Area Air Defense Command and Control

FM - Field Manual

FS-LIDS - Fixed Site-Low, Slow, Small Unmanned Aircraft System Integrated Defeat System

GNSS - Global navigation satellite system

GPS - Global Positioning System

HALE - High-altitude long endurance

HEL - High-energy laser

HEP - High explosive proximity

HPM - High-powered microwave

IFF - Identification Friend or Foe

IFPC - Indirect Fire Protection Capability

IR - Infrared

ISR - Intelligence, surveillance, and reconnaissance

JCO - Joint Counter-small Unmanned Aircraft Systems Office

JCU - Joint C-sUAS University

JP - Joint Publication

JUON - Joint Urgent Operational Need

LaWS - Laser Weapon System

LCEI - Low-collateral effects interceptors

LOS - Line of sight

L-MADIS - Light-Marine Air Defense Integrated System

LPWS - Land-Based Phalanx Weapon System

MALE - Medium-altitude long endurance

MCoE - Maneuver Center of Excellence

M-LIDS - Mobile-Low, Slow, Small Unmanned Aircraft Integrated Defeat System

MSL - Mean sea level

RCCTO - Rapid Capabilities and Critical Technologies Office

RF - Radio frequency

ROE - Rules of engagement

SHORAD - Short-range air defense

sUAS - Small uncrewed aerial systems

THAAD - Terminal High Altitude Area Defense

TIE - Technical Interoperability Exercise

TTPs - Tactics, Techniques, and Procedures

Contents

Key Findings	1
Introduction	3
<i>Research Scope and Objectives</i>	5
1 The sUAS Threat	6
<i>Defining sUAS</i>	7
<i>sUAS Missions and History</i>	10
<i>Global Proliferation</i>	12
<i>Future Threats</i>	16
2 Detecting and Defeating sUAS	18
<i>Sensors</i>	19
<i>Command and Control</i>	22
<i>Effectors</i>	24
<i>A Diverse Solution Set</i>	28
3 The Current Path	29
<i>Urgent Need</i>	30
<i>Refinement</i>	31
<i>Institutionalization</i>	33
<i>Doctrine</i>	34
<i>Organization</i>	35
<i>Training</i>	37
<i>Materiel</i>	39
<i>Leadership and Education</i>	39
<i>Personnel</i>	39
<i>Facilities</i>	41
Conclusion	42
Authors	44
Endnotes	45

Figures & Tables

Figure 1: Drone Evolution	4
Figure 2: Ukrainian Service Member Fires Rifle at Drone	7
Figure 3: Ukrainian Drone Minesweeper	11
Figure 4: The Path to sUAS Proliferation	13
Figure 5: Agricultural Drones	14
Figure 6: Drones in Formation	17
Figure 7: RADA Radar	20
Figure 8: The LIDS Family	23
Figure 9: Coyote Testing	25
Figure 10: Leonidas Pod HPM	25
Figure 11: Leonidas Ground-Based HPM	25
Figure 12: Dronebuster Training at the Baghdad Embassy Compound in Iraq	25
Figure 13: L-MADIS Training	25
Figure 14: High-Energy Laser Weapon Testing	25
Figure 15: Iranian-Made Kamikaze Drone	31
Figure 16: C-sUAS Milestones	32
Figure 17: JCO Demonstration at Yuma Proving Ground	37
Figure 18: Preparing RQ-7B Shadow for Flight	41
Table 1: U.S. UAS Classification	8
Table 2: NATO UAS Classification	9
Table 3: Select sUAS Combat Deployments	12
Table 4: DJI Development	14

Table 5: The Air Defense Kill Chain	19
Table 6: C-sUAS Platform Considerations	19
Table 7: C-sUAS Sensor Strengths and Weaknesses	21
Table 8: Example C-sUAS Effectors by Defeat Mechanism and Basing	24
Table 9: C-sUAS Effector Modality Strengths and Weaknesses	26
Table 10: Select C-sUAS Operations	28
Table 11: Air and Missile Threat Matrix	29
Table 12: DOTMLPF Plans and Potential Pitfalls	33
Table 13: Army C-sUAS Doctrine	35
Table 14: Major U.S. C-sUAS Training and Development	38
Table 15: C-sUAS Operator Frameworks	40

Key Findings

- For years, air defense has been the domain of specialized units and niche capabilities under conditions of air superiority. That era is no more, and the entire joint force must now look up. Small uncrewed aerial systems (sUAS) pose a significant threat, exhibiting multi-mission capabilities, minimal signatures, wide proliferation, low costs, and ground force utility. The common use of sUAS today amplifies other trends in modern warfare, including further complicating the airspace, saturating battlefields with more reconnaissance and strike assets, and expanding support for precision strike complexes. Their introduction is comparable to that of mortars and anti-tank missiles in the degree for which they have and will continue to push ground forces to adapt their tactics, techniques, and procedures.
- The mission and capabilities to counter sUAS (C-sUAS) should be shared across numerous unit types, including air defense, maneuver, support, and sustainment. The high demand and low density of air defense formations requires that air defenders and non-specialists work together as part of a combined arms for air defense (CAFAD) approach. The central question today, however, is the specific division of labor among the air defense and non-air defense units, as well as the authorities delegated to these groups. In general, C-sUAS planners have borrowed the distinction between “area” and “point” defense whereby traditional air defenders manage larger systems such as high-energy lasers and long-range kinetic interceptors for area defense, while maneuver forces use point defenses such as guns, nets, and handheld platforms.
- U.S. C-sUAS acquisition processes require updating to keep pace with evolving threats. The Joint Counter-small Unmanned Aircraft Systems Office (JCO) was stood up to coordinate

C-sUAS doctrine, organization, and training across the joint force. Congressional and Department of Defense (DoD) leadership should consider modifications to JCO's authorities and relation to service acquisition agencies to improve the requirements process and acquisition timelines.

- Air defense has multiple meanings and connotations, especially in terms of service-specific terminology. As a mission, air defense destroys, nullifies, or reduces the effectiveness of enemy attacks by aerial platforms. Defined organizationally, it connotes force structure responsibilities, such as the Army's Air Defense Artillery branch, or specific units manned, trained, and equipped to detect, track, and defeat aerial threats in specified sectors or altitudes. Because sUAS represent a distributed challenge to the entire joint force, C-sUAS operations cannot be confined to a single unit or specialization. C-sUAS developers, planners, and operators must overcome organizational silos.
- A variety of kinetic and non-kinetic capabilities are available to defeat sUAS. Over the past several years, the DoD has fielded a range of electronic attack and kinetic systems in support of joint and service urgent needs requests. Each of these tools have unique strengths and weaknesses in regard to survivability, range, magazine capacity, combat identification, and defended area.
- The institutionalization and propagation of C-sUAS capability will require developments across doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Training and capacity requirements will take priority over capability improvements over the next few years. New doctrine should specify the division of labor between air defense and non-air defense specialists, as well as the specific sensors, command and control, and effectors that they can operate. The policy, strategy, budget, and programmatic decisions made at this stage will carry enormous consequences for the field.

Introduction

Over the past decade, sUAS have become a core capability on the modern battlefield. Many are commercially sourced, easy to deploy, hard to detect, and highly proliferated. State and nonstate actors alike use them around the world in major conflicts, gray zone and criminal activities, and targeted killings. Technological advances in sUAS optics and sensor miniaturization have made them increasingly versatile as a primary reconnaissance tool, including for targeting for larger artillery and missile strikes. sUAS will continue to present a serious threat to military targets and civilian population centers.

Numerous studies have highlighted the sUAS threat.¹ A few have reviewed C-sUAS platforms and capabilities.² Yet to date, there appears to be no public-facing report that assesses C-sUAS history, strategy, and programs, across the DOTMLPF. This report tries to fill that gap from the perspective of the U.S. military.

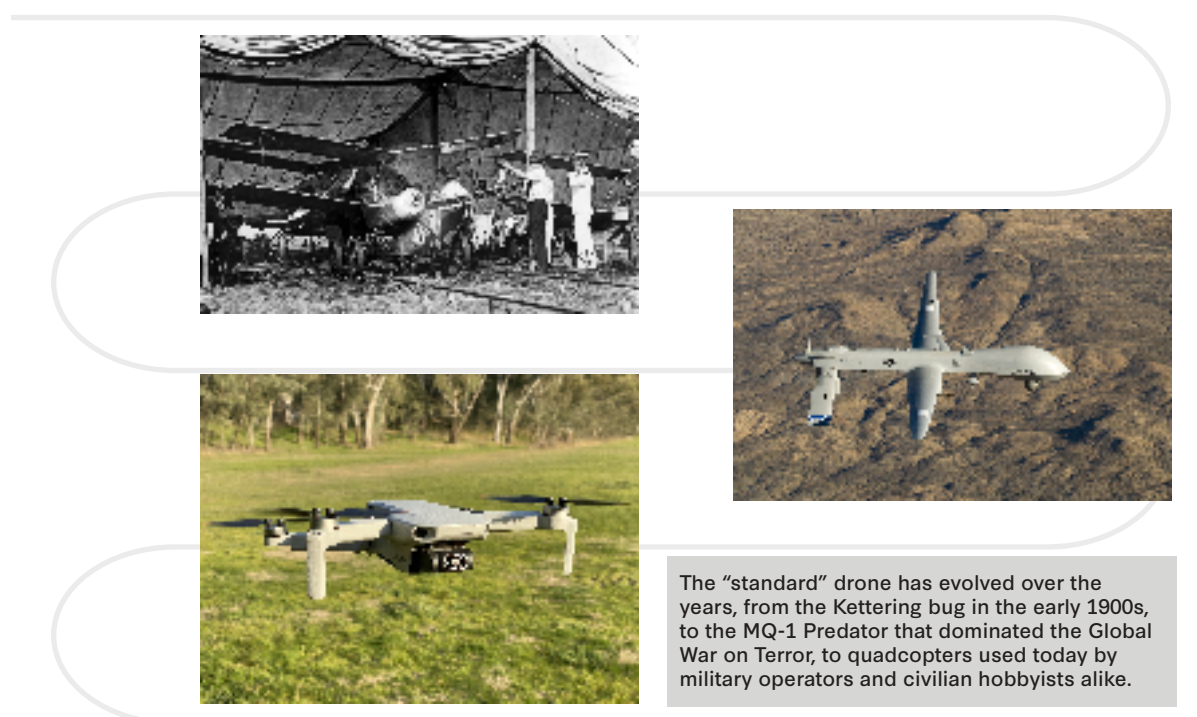
The C-sUAS mission is a challenging one. The threat is cheap and plentiful, whereas defenses are still emerging and bring significantly higher costs. Attribution can be difficult, complicating deterrence through retaliation. It remains unclear whether the active defense solutions currently in development will become programs of record; if investments in time, money, and personnel will continue to support this mission; and how well the multiple services involved can coordinate on developing and deploying their active defenses. While the U.S. Army is the lead service for developing joint doctrine, requirements, materiel, and training, the C-sUAS mission is not and must not be limited to one service, branch, or specialization. It is a concern for the entire joint force.

Air defense has continually evolved to meet new threats and challenges, from surveillance balloons to bomber aircraft to ballistic and cruise missiles. The threats have gotten smaller, harder to detect, and more sophisticated over time. At numerous moments along the way, a given threat will be deemed unstoppable—until, of course, defenses evolve to prove that assumption incorrect. C-sUAS represents the next chapter for the evolution of the air defense mission.

Fortunately, the DoD today recognizes the importance of C-sUAS. Nearly a decade ago, ISIS militants began using commercial quadcopters effectively in battle. In January 2020, the DoD established the JCO to rapidly prototype, test, demonstrate, and field new defenses. More recently, the Biden administration’s 2022 Missile Defense Review included C-UAS as a component of the defense against “missile-related” threats.³

With doctrine, organizations, materiel, training, and other issues under debate today, the United States and its allies face a critical period with sUAS and C-sUAS. High levels of sUAS proliferation, little to no regulatory oversight, and improved capabilities, technologies, and integration all converge to create an environment in which the U.S. military must respond to a rapidly evolving threat. Contributors to these conversations must understand the threat and its likely evolution, the defenses available and in development today, and the principles that should guide their application. For better or worse, the policies and institutions developed today will last for years to come.

Figure 1: Drone Evolution



Source: U.S. Army and Wikimedia Commons.⁴

Research Scope and Objectives

This report discusses current C-sUAS defenses used to detect and defeat small drones. It serves as a guide for understanding and evaluating C-sUAS solutions, both to inform policymakers by providing principles for future developments in this field, and to inform the public on a key defense issue for which there is a gap in the open-source literature. The report explores the trade-offs among various C-sUAS sensor and effector types but does not advocate for any particular solution set. It also does not address sUAS counterproliferation and regulation efforts, offensive “left-of-launch” strikes, camouflage, deception, signature management, nor other topics related to but not centered on active defense. Furthermore, it does not address specific operational or tactical issues, such as UAS notification procedures or how U.S. personnel should coordinate intercept engagements with allies. These processes are better addressed by U.S. military leaders as they update their related doctrine and standard operating procedures.

The study focuses closely on C-sUAS for the DoD, as primarily operated by the U.S. Army and Marine Corps. There are several other U.S. stakeholders in this field, including the Department of Justice, Department of Homeland Security, and the Federal Aviation Administration. The C-sUAS requirements, regulations, and resources differ among these groups.

This report uses the broad definition of air defense, which is to detect, track, and defeat aerial threats.⁵ It does not use the U.S. military’s organizational-specific definition of air defense as Air Defense Artillery or other groups specifically trained and equipped to detect, track, and defeat sophisticated air threats in large, specified sectors. sUAS break down the military’s typical distinction between air defense and force protection through their small size, wide proliferation, and flight patterns. C-sUAS will be a necessary part of both air defense and force protection, although there will be differing levels of operational expertise between trained air defenders and other military personnel.

The report has three sections. The first section aims to provide a brief analysis of the sUAS threat. It highlights common missions and capabilities through operational case studies and examines why sUAS have proliferated so quickly in recent years.

The second section reviews the ways and means to detect and defeat sUAS. This technology backgrounder broadly covers the sensors, C2, and effectors available today. This section reviews platforms that the DoD is pursuing and confirms the feasibility of C-sUAS technologies.

The third and final section lays out the U.S. C-sUAS development path from urgent need, to refinement, to institutionalization. As C-sUAS becomes institutionalized, there are opportunities and potential pitfalls across the DOTMLPF. The C-sUAS enterprise still faces unresolved questions regarding political authorities for C-sUAS stakeholders, personnel responsibilities, and acquisition policies to enable rapid development and procurement.

The sUAS Threat

sUAS pose a significant threat due to their multi-mission capabilities, minimal signatures, wide proliferation, low costs, and ground force utility.

In late December 2022, Russia launched a massive assault against Ukrainian infrastructure targeting multiple key regions including Kharkiv, Kyiv, Lviv, and Odesa. The first wave of attacks was conducted with cheap Iranian-made Shahed-136 drones. Ukrainian air force officials believe Russia used the drones to overwhelm air defenses before sending cruise missiles in a second wave of attacks.⁶ These attacks left several regions without power, including major cities such as Lviv and Kyiv.⁷ This incident was just one among many in a months-long strike campaign targeting Ukraine’s critical energy infrastructure in the hopes of demoralizing the public and leaving them without heating during the winter months.⁸

Today, sUAS are widely recognized as a ubiquitous, mature, and lethal part of the modern aerial threat spectrum. Their use in the Russia-Ukraine conflict is just one of many cases that have occurred over the past decade. Operators can attack adversaries with sUAS by dropping bombs or using the drone as a loitering munition in “kamikaze” suicide attacks. They can also conduct intelligence, surveillance, and reconnaissance (ISR) missions to collect information on an adversary’s position or activities. Modern sUAS sensors and data links can connect to larger kill chains or be used to find and fix targets for artillery and other precision-guided munitions. sUAS can conduct these missions while being difficult to detect and defeat with current air defenses.

Modern air and missile defenses are ill-suited to counter low-flying, slow, and small UAS. Following U.S. divestment from short-range air defense in the 1990s and early 2000s, the U.S. military has been challenged to respond to enemy sUAS.⁹ Other states have faced similar issues. In 2016, Israel fired two \$3 million PAC-2 interceptors and scrambled a fighter aircraft in a failed attempt to shoot

down a sUAS from Syria that had violated Israeli airspace.¹⁰ In its conflict with Yemen’s Houthis, Saudi Arabia used fighter aircraft to patrol the border and shoot down drones worth a few hundred dollars with \$2 million air-to-air missiles.¹¹ These responses are enormously costly and wasteful over longer military campaigns.

Figure 2: Ukrainian Service Member Fires Rifle at Drone



A Ukrainian serviceman fires his rifle at a drone flying above his position near Bakhmut on March 20, 2023.

Photo credit: Aris Messinis/AFP via Getty Images.

The lack of active C-sUAS opens a gap in modern air defense that combatants around the world are exploiting. There is no substitute. The complement to active C-sUAS—passive defense—is important but insufficient. The United States cannot harden all of its military bases against sUAS, and force distribution is ineffective against the large quantity and low costs of sUAS. The United States and its partners therefore must develop active and integrated defenses to mitigate these risks.






Defining sUAS

sUAS are a specific category of drones. This categorization, however, varies across countries and organizations, with two key taxonomies outlined by the United States and NATO. The DoD divides UAS into five categories based on their weight, speed, and altitude ceilings, with the “small” category comprising Groups 1, 2, and 3. Despite its designation as “small,” Group 3 UAS can still be quite large at up to 600 kg. NATO offers a slightly different categorization, with sUAS falling under its Class 1 and 2 categories.¹²

UAS categorization is further complicated by capability overlap with munitions. For example, the Iranian-made Shahed-136 is generally categorized as a Group 3 UAS, but it often operates as a one-way attack munition. The unique nature of the Shahed-136 thus cannot be simply captured by looking at a categorization that is determined solely on weight, speed, and altitude ceilings. The U.S. Tomahawk missile, specifically Block 4 and 5 variants, likewise blurs the line between UAS and missile. These variants offer loitering capabilities, but due to their one-way strike mission, they are not categorized as a UAS. The UAS spectrum is undoubtedly messy but attempts at distinguishing these threats—like all air threats—are still useful for defenders to quickly characterize capabilities.








This report applies the U.S. classification model of “sUAS” as encompassing Groups 1, 2, and 3.

Table 1: U.S. UAS Classification

Class	Definition	Description	Example
Group 1: Micro/Mini	Weighs 20 pounds or less and normally operates below 1,200 feet above ground level (AGL) at speeds less than 100 knots	<ul style="list-style-type: none"> Covers the smallest aircraft with low radar cross-sections Offers low range, endurance, and payload capabilities Widely available on the commercial market at low cost, with minimal logistical or personnel requirements 	DJI Phantom 3 
Group 2: Small Tactical	Weighs 21 to 55 pounds and normally operates below 3,500 feet AGL at speeds less than 250 knots	<ul style="list-style-type: none"> Covers larger and more capable aircraft than Group 1, but still widely available on the commercial market Offers enhanced range, endurance, and payload capabilities 	Orlan-10 
Group 3: Tactical	Weighs between 55 and 1,320 pounds, and normally operates below 18,000 feet mean sea level (MSL) at speeds less than 250 knots	<ul style="list-style-type: none"> Covers a wide array of aircraft with significant differences across range, endurance, payload, and size Carries a larger logistical burden than Groups 1 and 2; generally reserved for military or commercial shipping purposes 	Forpost 
Group 4: Persistent	Weighs more than 1,320 pounds and normally operates below 18,000 feet MSL at any speed	<ul style="list-style-type: none"> Covers the largest aircraft operating at medium to high altitudes Offers significant range, endurance, and payload capabilities Carries a heavy logistical burden, similar to that of manned aircraft 	Yilong 1 
Group 5: Penetrating	Weighs more than 1,320 pounds and normally operates higher than 18,000 feet MSL at any speed	<ul style="list-style-type: none"> Covers the largest aircraft operating at high altitudes Offers the greatest range, endurance, and payload capabilities Carries a heavy logistical burden, similar to that of manned aircraft 	BZK-005 

Source: Classifications from U.S. Army; images from Russian Ministry of Defense and Wikimedia Commons.¹³

Table 2: NATO UAS Classification

Class	Category	Employment	Operating Altitude	Mission Radius	Command Level	Example
Class I (<150 kg)	Micro (<66 J)	Tactical Sub-unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km; line of sight (LOS)	Platoon, Squad	Black Widow 
	Mini (<15 kg)	Tactical Sub-unit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company, Platoon, Squad	Skylark 
	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion, Regiment	Scan Eagle 
Class II (150 kg – 600 kg)	Tactical	Tactical Formation	Up to 18,000 ft AGL	200 km (LOS)	Brigade	Hermes 450 
Class III (>600 kg)	MALE	Operational/Theatre	Up to 45,000 ft MSL	Variable; beyond line of sight (BLOS)	Joint Task Force	Heron 
	HALE	Strategic/National	Up to 65,000 ft MSL	Variable (BLOS)	Theatre	Global Hawk 
	Strike/Combat	Strategic/National	Up to 65,000 ft MSL	Variable (BLOS)	Theatre	Reaper 

Source: Classifications from NATO; images from Vulcan UAS, Elbit Systems, Wikimedia Commons, and U.S. Department of Defense.¹⁴

sUAS have several advantages over larger aircraft, both crewed and uncrewed:

1. **Lower cost:** sUAS are relatively inexpensive compared to larger aircraft. This is true even when platforms are not quite “consumable” aircraft that operators will only use on a single mission.
2. **Low training burdens:** sUAS operators can learn their basic tradecraft in hours, and only one person is needed to operate a drone. On the other hand, it takes months to years to train pilots on large aircraft—including uncrewed platforms such as the MQ-9. A single platform may require over 100 personnel for operations and maintenance.¹⁵
3. **Minimal infrastructure requirements:** Unlike larger aircraft, sUAS do not require extensive infrastructure to deploy such as long runways, secure and complicated data links, or expensive maintenance equipment.
4. **Gray zone applications:** Combatants frequently employ sUAS to decrease the perceived political costs and escalation risks resulting from operations and potential shootdowns as compared to larger, inhabited aircraft.¹⁶ The low-cost of sUAS, minimized risk to operators (on the ground rather than in the cockpit), and difficulty of attribution make sUAS a useful tool for gray zone operations.
5. **Unique capabilities in modern warfare:** sUAS can perform an increasing number of air missions at lower cost than large, crewed aircraft. Small loitering munitions offer the ability to scan large swaths of territory and quickly strike targets of interest. Medium- and high-altitude long endurance (MALE/HALE) drones will continue to play an important role in counterterrorism missions, but they appear less effective in symmetric, conventional conflicts.¹⁷ Looking to the future, sUAS swarms may also provide a cost-effective means to saturate an adversary’s air defenses.

To be sure, sUAS also have critical disadvantages over larger aircraft.

1. **Limited payload capacity:** sUAS are unable to carry heavier, more capable sensors or explosives.
2. **Limited flight duration and range:** Commercial sUAS can perhaps fly around 8 km at the high end. Military sUAS may feature extended ranges, but they will not approach large aircraft ranges.
3. **Limited operating conditions:** Compared to larger aircraft or missiles, sUAS are more susceptible to wind and adverse weather conditions, as well as a greater diversity of active defenses. Ukraine, for example, is reportedly losing around 10,000 sUAS per month against Russia.¹⁸

sUAS Missions and History

sUAS can complete the same missions as manned aircraft. Over the past decade, military operators have used sUAS for six primary missions:

- **Attack operations:** Strikes on people and things with bombs, missiles, or suicide attacks

- **Intelligence, surveillance, and reconnaissance:** Providing “eyes in the sky” for military planning and operations
- **Targeting:** Finding and sharing target location with other strike assets, such as artillery
- **Battle damage assessment:** Confirming the results of an attack
- **Harassment:** Creating confusion and alarm with drone incursions, possibly including small attacks
- **Propaganda:** Showing off military platforms and operations to improve military and civilian morale

Attack operations, ISR, and targeting missions are the most common, as clearly shown in the Russia-Ukraine war. Both sides have used sUAS to search for enemy combatants and either target them directly or pass their location to other strike assets such as artillery to fire upon their position. Ukrainian soldiers have used the U.S. Switchblade and Phoenix Ghost UAS, for example, to directly target Russian tanks and personnel.¹⁹ Early failures in the war also prompted Russia to quickly increase the use of stand-off weaponry, including indigenous and foreign-made sUAS such as the Lancet-3 and Shahed-136, respectively.²⁰ In general, the Russia-Ukraine war highlights how sUAS have enabled complex, integrated air attack through the wide proliferation of sensors. As others have warned about the modern battlefield, “What can be seen can be hit, and what can be hit can be destroyed.”²¹

Figure 3: Ukrainian Drone Minesweeper



UAS operators use drones for various missions outside of the six described above. Here a Ukrainian volunteer controls the flight of a drone carrying a metal detector to search for mines near the town of Derhachi, Kharkiv region, on October 1, 2023.

Photo Credit: Sergey Bobok/AFP via Getty Images.

Attack operations also include strikes on infrastructure and economic targets. In September 2019, Iran launched 18 sUAS and seven missiles to attack Saudi Arabian oil facilities in Abqaiq and Khurais.²² The strike successfully evaded Saudi air defenses, including the U.S. Patriot, German Skyguard, and French Crotale, and struck their targets, leading Saudi Arabia to temporarily cut oil production by around 50 percent.²³ In Ukraine, Russia has launched Iranian-made suicide drones to strike power grids.²⁴

sUAS-based assassination attempts—and successes—have also rocked several countries. In August 2018, a small insurgency group in Venezuela used a bomb-laden drone in a failed assassination attempt against President Nicolás Maduro.²⁵ In January 2019, the Houthis in Yemen used a Qasef-1 UAS to assassinate senior Yemeni military officials.²⁶ More recently in November 2021, Iranian-backed militias attempted to assassinate Iraqi prime minister Mustafa al-Kadhimi after pro-Iran political groups had faced disappointing results in the elections.²⁷

Harassment and propaganda operations are also common. ISIS fighters made extensive use of commercial quadcopters and fixed-wing drones for surveillance, propaganda, and small but demoralizing tactical strikes.²⁸ In January 2017, despite having a limited sUAS arsenal, the group formally announced a new drone unit known as “Unmanned Aircraft of the Mujahideen.”²⁹ In the 2020 Nagorno-Karabakh war, Azerbaijan used its drone fleet to record video of its strikes against Armenian tanks and soldiers, replaying footage across the country and internationally.³⁰ Iranian-backed groups have frequently launched sUAS and rocket attacks to harass U.S. embassies, businesses, and military personnel across the Middle East, which has occasionally led to counterattacks and rising escalation concerns.³¹

Table 3: Select sUAS Combat Deployments

Operator	Conflict	Platforms
Houthis	Yemen civil war (2014–present)	Iranian Shahed-136, Iranian-derived Qasef-1, and commercial drones
ISIS	Iraqi civil war (2016–2018)	Commercial drones
Boko Haram	Attacks on Nigeria and Cameroon (2018–present)	Commercial drones
Azerbaijan	Nagorno-Karabakh war (2020)	Israeli Harop, Orbiter-1K; Turkish Bayraktar TB2
Russia	Russian invasion of Ukraine (2022–present)	Russian Orlan-10, Lancet-3, and Forpost; Chinese DJI commercial drones; Iranian Shahed-136
Ukraine	Russian invasion of Ukraine (2022–present)	U.S. Phoenix Ghost, Switchblade 300; Turkish Bayraktar TB2; Chinese DJI commercial platforms

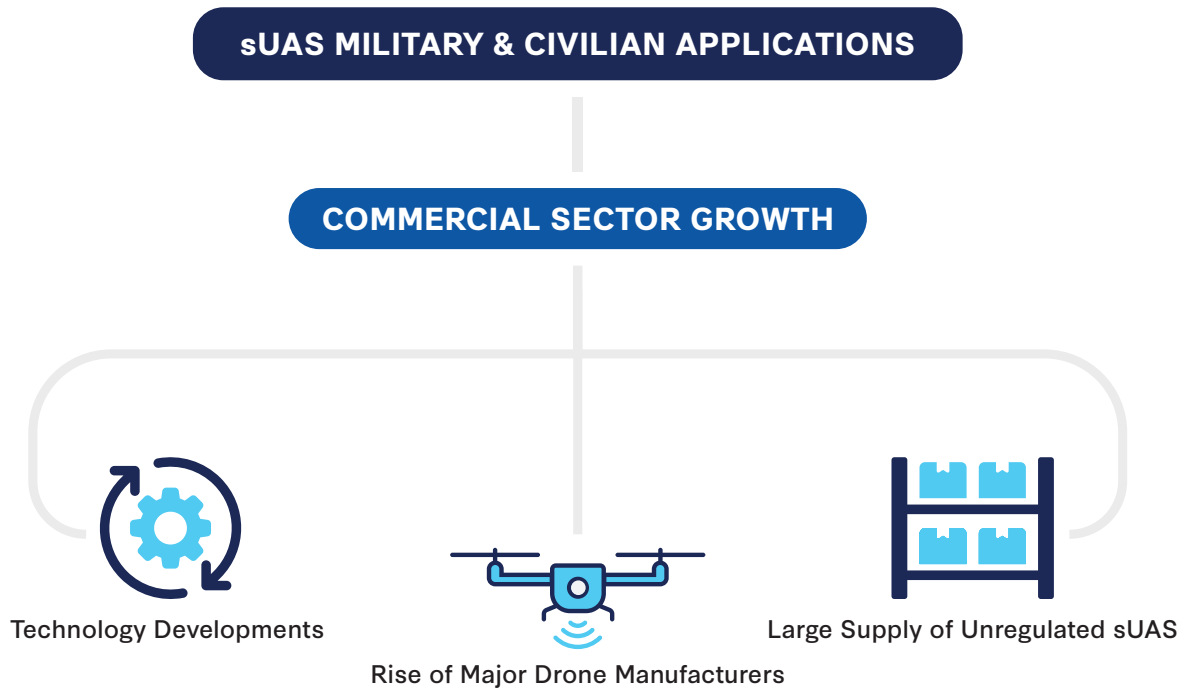
Source: CSIS Missile Defense Project.

Global Proliferation

sUAS have spread globally over the past decade due to the technology’s dual use for both military and civilian applications. In addition to the military missions listed in the previous section, sUAS are used in various civilian activities, including filmmaking, law enforcement, emergency response, agriculture, delivery, and the protection of commercial facilities. Once sUAS technology advanced enough to become viable for these use cases, the commercial market boomed, which in

turn has further fueled sUAS technology developments, facilitated the rise of commercial drone manufacturers, and created a massive, largely unregulated supply of these aircraft.

Figure 4: The Path to sUAS Proliferation



Source: CSIS Missile Defense Project.

Before the sUAS commercialization boom of the mid-2010s, manufacturers created moderately priced units with relatively rudimentary capabilities. The first remote-controlled drone to incorporate Wi-Fi, Parrot's A.R. Drone, was released in 2010 and cost a modest \$299 but had a battery life of only 12 minutes. Three years later Da-Jiang Innovations (DJI), the current commercial manufacturing titan in China, released its first drone, the Phantom 1, which sold for \$379.³² This model featured an internal GPS but had a flight time of less than 10 minutes and a communication distance of only 1 km.³³ Today, the cost of commercial sUAS has increased, typically ranging from \$500 to \$10,000, but new models offer significantly improved capabilities.³⁴ DJI's bestselling Mavic 3, which costs \$2,049, offers 46 minutes of flight time, omnidirectional obstacle sensing, and a transmission range of 15 km at 1080p resolution. The cost-to-flight-time ratio between these DJI models increased by 17.5 percent, but the capabilities provided by the Mavic 3 opened the door to hundreds of commercial and hobbyist applications.

China has since seized the sUAS market, with DJI accounting for over 60 percent of the market share for commercial sUAS in 2021.³⁵ While market projections for commercial drones vary slightly, there is strong consensus that the market is thriving and shows no signs of slowing down, as exemplified by revenue of \$2.7 billion in 2020 and a projected intake of \$21.7 billion by 2030.³⁶

Table 4: DJI Development

	Release Year	Max Distance	Max Speed	Battery Type	Battery Power	Price
DJI Phantom	2013	1 km	10 m/s	Li-Po	20 W	\$379
DJI Mavic 3	2022	30 km	5 m/s (C mode)	Li-ion 4S	65 W	\$2,049
			15 m/s (N mode)			
			21 m/s (S mode)			

Source: DJI.³⁷

The commercial drone sector has driven technological advances, rather than these advances trickling down from military UAS. This growth has mostly been spurred on by the smartphone industry. Radio-controlled aircraft moved from using petrol engines to electric motors and the lithium batteries used in modern smartphones. With internal combustion engines prone to excessive vibration, electric motors have become increasingly popular, particularly for sUAS.³⁸ Critically, the extensive lithium battery market has allowed operators to choose battery packs that fit their desired performance, flight time, and endurance without massive price increases. The recent interest in and testing of UAS-compatible lithium-sulfur batteries may offer an even cheaper option in the coming years.³⁹ The leveraging of existing high-speed cellular networks has also allowed for broader UAS accessibility and lower associated costs. Overall, as one expert aptly explained, “Drones have really been riding the smartphone revolution.”⁴⁰

Figure 5: Agricultural Drones



A Kenya Airways employee controls a drone as it spreads fertilizer over a tea farm at Kipkebe Tea Estate in Musereita on October 21, 2022.

Photo Credit: Patrick Meinhardt/AFP via Getty Images.

The military sUAS market has similarly increased in size and platform diversity over the last decade. There is limited reporting specifically on sUAS market trends, but the wider military UAS market features many Groups 2 and 3 platforms and shows clear signs of rapid expansion. Between 2011 and 2021, the military UAS market grew by nearly \$10 billion, from \$1.7 billion to \$11.6 billion.⁴¹ As commercial markets and systems proliferated, indigenous military programs also promptly appeared, offering to enhance and counter the new technological capabilities available. An October 2020 study estimated that 102 countries possessed an active drone program compared to an estimated 60 countries in 2010.⁴² Additionally, of the reported 171 active military drone models in 2019, roughly 143 were sUAS.⁴³ Militaries have also successfully harnessed the cheap and easy-to-use format of commercial systems while increasing the reliability and security needed for military operations.⁴⁴

The general utility of sUAS reinforce their proliferation. Russia has imported the Iranian Shahed-136 in large numbers to support its operations in Ukraine while also relying on domestic systems such as the Orlan-10. Prior to its operations in Nagorno-Karabakh, Azerbaijan procured large numbers of Israeli sUAS, which Azerbaijani operators used effectively against Armenian combatants. Growing normalization of sUAS as tools of war points toward a shifting military landscape in which sUAS will regularly be relied upon in order to achieve mission success.

Given the wide commercial and civilian applications of sUAS, international regulatory efforts to stem sUAS proliferation have fallen short. In October 2016, 53 nations, including the United States, issued a joint declaration that attempted to start the process of building a basic framework for international UAS standards, but it failed to spur meaningful action.⁴⁵ A framework demanding sUAS buyers and sellers to comply to specific obligations had the potential to hinder exports and create strains with legitimate trading partners.⁴⁶ In addition, China's absence from the declaration inhibited its possibility of success from the start. Having taken control of a significant share of the global UAS market, Beijing was, and continues to be, unlikely to allow any regulation that negatively affects its exports.

Even if a regulatory body were established, it is unclear how helpful it would be in removing sUAS from modern battlefields. Clear rules for manufacturers or regulations on military sUAS transfers would not decrease the wide availability of commercial drones or components of these systems, which can easily be adapted for military use even by non-state actors. According to a 2018 West Point report, ISIS displayed overall diversification within its commercial drone supply chain. For the nine quadcopters associated with ISIS operations, engineers built the final units after acquiring various components from seven retailers in five different countries.⁴⁷ ISIS's piecemeal production of UAS is also not an isolated practice. The Houthis in Yemen follow a similar pattern. For example, the Sammad-pattern UAS engine originated in Germany before making its way to Israel, then Iran, and eventually into the hands of Houthi engineers in Yemen.⁴⁸ Given this substantial supply of cheap components spread across multiple business sectors, and the ease with which it crosses international borders, increasing regulations around sUAS is unlikely to stem proliferation and use.

As sUAS continue to develop and improve upon existing capabilities within the civilian and commercial markets, potential applications have continued to grow. There is little chance of putting the genie back in the bottle. The United States and its allies must develop active defenses

to address these highly proliferated systems and deploy them as required based on expected risks and vulnerabilities.

Future Threats

Technological developments over the next few years will further empower sUAS. The rise of artificial intelligence and machine learning (AI/ML) is perhaps the most common concern. As the JCO warned in their 2021 report: “The impending integration of artificial intelligence with autonomous sUAS will introduce yet another dramatic change to the character of warfare.”⁴⁹ Software is already enabling rapid leaps in UAS autonomy. As one CSIS report explains:

Traditional software is sufficient to deliver a high degree of autonomy for some military applications. For example, the Israeli Aerospace Industries (IAI) Harpy is a decades-old uncrewed drone that IAI openly acknowledges is an autonomous weapon. When in autonomous mode, the Harpy loiters over a given region for up to nine hours, waiting to detect electromagnetic emissions consistent with an onboard library of enemy radar, homes in on the emissions source (usually enemy air defense radar), and attacks. No human in the loop is required.⁵⁰

As these autonomous capabilities proliferate further, defenders will be forced to pivot away from detect and defeat platforms based on radio frequency (RF).⁵¹

Advances in AI/ML may also enable sUAS swarms. These are large, coordinated, and at least semi-autonomous group operations; thus far, there have been few if any attacks that fit this strict definition. Yet even small, human-controlled group attacks have proven capable. The 2019 Houthi attack on two Saudi Aramco oil facilities only employed 10 drones but still degraded business operations for some time. Commercial drone shows have operated with more than 3,000 drones.⁵² Once mass drone swarm technology is established, it will be an increasingly difficult threat to intercept. In those cases, the best options for defenders may be “left-of-launch” strikes on C2 nodes and ground control stations associated with the attack.

Adversary sUAS may increasingly communicate through cell towers, making RF-based detect and defeat difficult. Under this environment, defenses would need to differentiate between sUAS communications and regular cellular transmissions. Even if sensors can adapt, RF-based defeat would then need to degrade those communications without disrupting cellular transmissions using those same frequencies. As JCO director Sean Gainey explained in 2022, sUAS operators are “building in redundancy in these systems where if you cut off something, they can fall back on something else.”⁵³

Lastly, U.S. policymakers must also prepare for creative sUAS use in the battlefield. In the 2020 Nagorno-Karabakh war, for example, Azerbaijan reportedly modified older aircraft to function uncrewed and used these aircraft to draw fire and locate Armenian air defenses. Russia has used similar tactics in its ongoing invasion of Ukraine. Russian operators have also developed tactics such as piloting near buildings to exploit sensor blind spots, launching UAS away from operator locations

to avoid counterattacks, and spoofing Ukrainian defenses to falsely register a large number of UAS and ground control stations.⁵⁴ UAS operators have enormous freedom of action and can adapt tactics quickly, whereas defenders typically do not have such flexibility.

Figure 6: Drones in Formation



South Korea's military drones fly in formation during a South Korea-U.S. joint military drill at Seungjin Fire Training Field in Pocheon on May 25, 2023.

Photo Credit: Yelim Lee/AFP via Getty Images.

Detecting and Defeating sUAS

A variety of kinetic and non-kinetic capabilities are available to defeat sUAS. Each of these tools have unique strengths and weaknesses in regard to survivability, range, magazine capacity, combat identification, and defended area.

SUAS pose unique challenges to air defense. They exploit gaps in sensing because they are small and fly low. They also exploit cost asymmetries—they are usually cheap and numerous, while air defense interceptors are not. They even exploit the way air defense is organized by equipping individual combatants to achieve tactical and strategic effects, while the United States and its allies mostly deploy air defense at the company level or higher.

Despite these differences across size, flight, costs, and quantities, the overall air defense kill chain is essentially the same. Air defense—as defined broadly—means detecting and defeating airborne threats flying from surface to space. That process can be illustrated in various ways, as shown in Table 5. The sensors, effectors, and C2 platforms involved in this kill chain all have unique characteristics that determine their effectiveness and where they are deployed, as shown in Table 6.

The following sections define the sensor, effector, and C2 missions, and explore different C-sUAS modalities, their respective strengths and weaknesses, and example platforms for each.

Table 5: The Air Defense Kill Chain

Detect		Track	Identify
1: Warning	2: Custody	3: Track/Identify/Pair	4: Decision Time
Detection of unidentified air objects	Wide-area surveillance maintains custody of threats as they transit	Tracking and identifying threats and pairing them with engagement options	Human authorities confirm a hostile threat, communicate to leaders, decide whether to engage, and select an intercept option
Engage			
5: Effector Deployed	6: Engagement	7: Assess and Reengage	
Authorities communicate the engagement decision and deploy the air defense effector	Effector deploys and contacts the threat	Assessing target engagement and deploying another effector, if necessary and possible	

Source: CSIS Missile Defense Project.

Table 6: C-sUAS Platform Considerations

General	Requirements	Operational Context
Cost: How much does it cost to develop, deploy, and operate?	Basing: Is it fixed or semi-fixed, mounted or mobile, and dismantled or handheld?	Collateral: Does it work safely in populated areas? Does it work near airports or in other RF-dense environments?
Technology Readiness Level: Is it ready to deploy today? How much time and money must be invested before operational use is feasible?	Logistics: What are the transportation and personnel requirements for deployment, operations, and maintenance? How long does it take to deploy?	Echelon: Is it designed to equip a small, medium, or large unit?
Integration: Does it work and communicate with deployed sensors, effectors, and C2?	Training: How long does it take to become operationally proficient?	

Source: CSIS Missile Defense Project.

Sensors

Radar has long been the primary sensor used to detect and track aerial threats. The traditional approach leverages wide-area surveillance radars and highly focused tracking radars to respectively detect and track incoming aircraft and ballistic missiles. Detecting sUAS in this way, however, is hard. As mentioned earlier, sUAS typically fly below typical air defense radar coverage. Perhaps even more problematic is their slow speeds and small profile, which combined creates a very limited radar signature for detection and tracking.

This is not to say that active radar does not work against sUAS. Active radar remains one of the predominant means for detecting sUAS at longer ranges as compared to other sensor modalities. Radar is also more capable under adverse weather conditions and less sensitive to countermeasures compared to other sensors.⁵⁵ Radars, however, can be large, heavy, and power intensive, thereby reducing mobility unless mounted on a vehicle.⁵⁶ They also emit a signature that can be easily

detected, making the operator's location vulnerable to attack. Radars also must be optimized to see smaller objects, thus reducing their detection range.

Another common method to detect sUAS today is electronic surveillance measures, also known as passive radio frequency. This detection method allows defenders to identify the wireless signals used to control the UAS.⁵⁷ Some passive RF capabilities show the location of both the sUAS and the operator. As one Department of Homeland Security report explains, C-sUAS may “use libraries of known UAS radio signatures and compare detected signals to those in the library in order to classify or identify UAS.”⁵⁸ These sensors listen to sUAS communications via control stations, satellites, cell towers, or drone relays. A key concern with passive RF, however, is that sUAS are moving away from RF control, making current detection and defeat capabilities obsolete.

Figure 7: RADA Radar






Source: DRS.⁵⁹



Due to the detection liability of radar, C-sUAS designers often seek to combine RF detection and radars within a single platform. The FS-LIDS (Fixed Site-Low, Slow, Small Unmanned Aircraft System Integrated Defeat System) is an example of a system supported by the JCO that incorporates both

detection methods.⁶⁰ The multi-layer detection capabilities of FS-LIDS allow operators to better conduct countermeasures that align with the given target and environment. However, a combination of sensors is not a necessity. EnforceAir is another JCO-supported system that uses RF for both detection and defeat.⁶¹ Nevertheless, sUAS operators can adapt to RF sensors. In July 2022, for example, a British defense firm developed a laser-controlled drone that will be undetectable by current RF sensors.⁶² Suicide drones, also known as one-way attack munitions or loitering munitions, may use an onboard inertial navigation system to allow sUAS to operate without alerting RF sensors. Russia has extensively used the Iranian Shahed-136 drone as a loitering munition in attacks on Ukraine.

Other sensor modalities include electro-optical (EO), infrared (IR), and acoustic sensors to detect a target by its visual, heat, or sound signatures, respectively. These sensors are helpful in providing additional confirmation of a nearby sUAS threat but are rarely used as a standalone sensor. EO, IR, and acoustic sensors have very limited operational ranges. For example, the EnforceAir’s RF sensor has a radius of approximately 3 km, while the Discovair G2 acoustic sensor has an estimated range of 500 m. Additionally, potential countermeasures are fairly simple, including, for example, flooding a battlefield with noise that degrades acoustic sensor capabilities. For these reasons, EO, IR, and acoustic sensors are often used in combination with active or passive radar to provide a more effective, layered detection capability.

Table 7: C-sUAS Sensor Strengths and Weaknesses

Mode	Characteristics	Example
Radar	<ul style="list-style-type: none"> • Mature technology, concepts of operations, and industrial base • Can be built to detect and track targets at long ranges • Can be built for all-weather capability • Active sensor; emits radio waves which can be detected 	FS-LIDS
		
Infrared (IR)/ Electro-Optical (EO)	<ul style="list-style-type: none"> • Imaging capability allows visual confirmation of incoming threat • Detection range affected by weather • Visual-spectrum EO sensors limited in nighttime operations • Passive sensor; difficult to localize and attack 	LPWS (EO)
		 M-LIDS (IR) 

Acoustic	<ul style="list-style-type: none"> • Ability to identify different types of UAS by cataloging unique audio signatures • Sound pollution, weather can degrade performance • Relatively limited range • Passive sensor 	<p>Discovair</p> 
Passive Radio Frequency	<ul style="list-style-type: none"> • Can detect and locate UAS ground control stations and related assets • Best option to identify and classify UAS • Cannot detect autonomous or non-emitting UAS • Passive sensor; detects radio emissions from UAS 	<p>EnforceAir</p> 

Source: Characteristics from Department of Homeland Security; images from SRC Technologies, U.S. Department of Defense, Squarehead Technologies, and D-Fend Solutions.⁶³

Command and Control

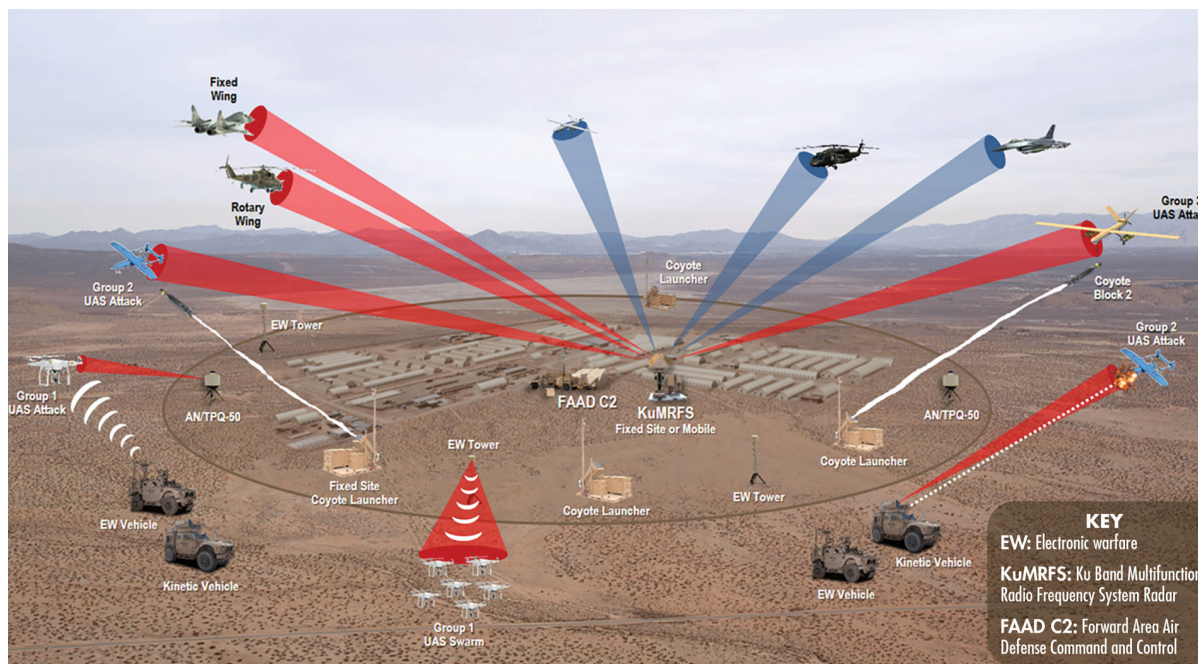
Command and control (C2) is a critical element of C-sUAS operations, as it is for all air defense. Broadly speaking, C2 is the “exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.”⁶⁴ A fundamental element of C-sUAS C2 is the centralized development of operational procedures that will enable decentralized execution of C-sUAS operations. Execution of the C-sUAS mission, in the near term, will be localized to the threatened asset or unit, and engagement authority will rest with the local commander and possibly junior leaders, who will make decisions based on the predefined rules of engagement. These tasks include integrating sensor data (from sources such as radar, cameras, and direction finders), classifying and identifying incoming threats, and transmitting this information among sensors and shooters to queue up responses. C2 operations require the creation of a common operational picture and share that intelligence with all relevant stakeholders.

While detecting sUAS presents the most commonly identified challenge, as previously discussed, sUAS also present a significant identification challenge. Over the near term, identification will depend more on context or procedures than specific Identification Friend or Foe (IFF) systems that confirm an sUAS’s affiliation. As a Joint Staff report explains, many U.S. UAS “do not have IFF capability and are similar or identical to threat [UAS].”⁶⁵ C-sUAS rules of engagement (ROE) will therefore depend on the operational environment and threat intelligence, with ROE able to tighten or loosen as necessary. Future C-sUAS platforms may feature improved non-cooperative threat recognition capabilities, but for now ROE will determine whether defenders can shoot at incoming sUAS rather than pursue the identification of the object.

C2 for C-sUAS has improved significantly over the past few years, becoming increasingly open and interoperable. In July 2020, the DoD designated the Forward Area Air Defense Command and Control (FAAD C2) system as the interim C2 system for C-sUAS. The FAAD C2 system provides a single integrated air picture that combines a suite of sensors, effectors, and other C2 systems given operational requirements.⁶⁶ JCO director Sean Gainey noted the superiority of the FAAD C2 compared to alternatives, specifically noting its fire control capabilities.⁶⁷ The rapidly evolving C-sUAS threat requires C2 development to build upon FAAD C2's successes. The ultimate goal, in the eyes of Gainey and the JCO writ large, is to create an "open architecture standard based C2 system" that can be configured according to specific threat analysis.⁶⁸

The current functions of FAAD C2 thus reveal the baseline of JCO C2 development. Currently FAAD C2 is hosted on a SRNC-17 laptop computer and Dell 7212 tablet computer, emphasizing the need for portable command functions. The extensive integration with sensors and communication systems also highlights the need for mature joint operation potential. FAAD C2 is deployed and integrated with 25 sensors, including AN/MPG-64 Sentinel and Ku-band Radio Frequency System (KuRFS) radars, and five communications systems, including Link 16 and Joint Range Extension Application Protocol.⁶⁹

Figure 8: The LIDS Family



The LIDS family of systems uses a range of passive and active sensors to detect, track, and identify UAS and non-hostile aircraft.

Source: U.S. Army Acquisition Support Center.⁷⁰

Effectors

The DoD has developed a variety of kinetic, directed energy, and RF-based defenses against sUAS. These tools all come with their own strengths and weaknesses. As is constantly repeated in the C-sUAS community, there is no “silver bullet” effector to defeat these threats.

Table 8: Example C-sUAS Effectors by Defeat Mechanism and Basing

	KINETIC			NON-KINETIC		
		Hard Kill		Hard Kill	Soft Kill	
	Missiles/ Drones	Guns	Entanglements	Lasers	Microwaves	Radio Frequency
Fixed/Semi-fixed	Anvil: Collision drone	Land-Based Phalanx Weapon System (LPWS): 20 mm ballistic round	Drone Hunter: Net capture	CLWS: High-energy laser	THOR: High-power microwave	FS-LIDS: RF/GPS
Mounted/Mobile	M-LIDS: Coyote collision drone	Stryker: 30 mm ballistic round	Drone Catcher: Net capture	M-SHORAD: High-energy laser	Leonidas: High-power microwave	L-MADIS: RF/GPS
Dismounted/Handheld		SMASH 2000L: Gun with laser rangefinder	Skynet: Net capture			Dronebuster: RF/GPS

Note: Many systems listed here feature multiple deployment configurations and effectors. This table is illustrative and not comprehensive, intended to show the range of C-sUAS on the market.

Source: CSIS Missile Defense Project.

Kinetic defenses include guns, nets, ropes, collision drones, missiles with proximity-fuse warheads, as well as more creative solutions such as falcons and strings of streamers to tangle propellers. Kinetic defenses typically employ mature technologies, offer the highest probability of kill for any single UAS, and allow significant range of intercept. Their weaknesses include vulnerability to sUAS swarms, given their focus on defeating individual drones. They also may be inappropriate for use in populated areas where intercept shrapnel may fall on people or property.

The DoD has invested in several kinetic effectors. The Coyote system is one of the primary interim solutions today.⁷¹ There are several extant configurations which may be characterized as a missile or drone, with a jet-engine to accelerate the system out of its launcher, and fins that support its loitering capability. The original Coyote entered demonstration testing in 2016 and employed a kinetic effect through collision or the nearby explosion of the unit’s warhead. According to its FY 2024 budget, the Army procured over 1,200 Coyote interceptors between 2022 and 2023.⁷²

The United States has steadily improved upon C-sUAS cost asymmetries. Given the proliferation of suicide drones such as the Iranian Shahed-136, which costs roughly \$20,000-50,000 per unit, using missile interceptors that cost two to eight times as much is deeply inefficient.⁷³ Instead, there has been a rise of cheaper alternatives such as anti-aircraft guns for C-sUAS, commonly known as “flak.” Ukraine, for example, has procured Germany’s Gepard self-propelled anti-aircraft gun, which can shoot down sUAS with a range of around 5 km, as well as the older Soviet ZU-23 anti-aircraft gun.⁷⁴ The DoD has also invested in an anti-drone “strings of streamers” system and is pushing the system into a program of record. These older, simpler technologies have proven effective against sUAS threats.



Source: Raytheon.⁷⁵

Figure 9: Coyote Testing

Figure 10: Leonidas Pod HPM



Source: Epirus.⁷⁶



Source: Epirus, Inc.⁷⁷

Figure 11: Leonidas Ground-Based HPM

Figure 12: Dronebuster Training at the Baghdad Embassy Compound in Iraq



Source: U.S. Department of Defense.⁷⁸



Source: U.S. Marine Corps.⁷⁹






Figure 13: L-MADIS Training

Figure 14: High-Energy Laser Weapon Testing



Source: U.S. Air Force.⁸⁰

Table 9: C-sUAS Effector Modality Strengths and Weaknesses

Mode	Characteristics	Example
Kinetics	<ul style="list-style-type: none"> • Mature technology, concepts of operations, and industrial base • Mixed characteristics based on munition: <ul style="list-style-type: none"> • Missiles and Collision Drones: Generally long-range, accurate if equipped with terminal guidance, and high cost per intercept • Guns and Entanglement: Limited range, lower accuracy, and lower cost per intercept 	<p>Anvil</p>  <p>Land-Based Phalanx Weapons System</p> 
	<ul style="list-style-type: none"> • Less technologically mature than kinetics • Lower cost per shot; high up-front costs • Atmospheric conditions can reduce system effectiveness • Two categories of DE weapons: <ul style="list-style-type: none"> • High-Energy Laser: Rapid, precise engagements that are limited to line-of-sight targets and can only attack one target at a time • High-Power-Microwave: Rapid engagement with anti-swarm capability, but limited range due to beam diffusion, and limited effectiveness against hardened targets 	<p>M-SHORAD</p>  <p>THOR</p> 
Electronic Warfare and Radio Frequency Jamming	<ul style="list-style-type: none"> • Mature technology • Low cost per intercept • Can forcibly land UAS intact • No effect on autonomous or non-communicative UAS 	<p>L-MADIS</p> 

Source: CSIS Missile Defense Project, images from Anduril and U.S. Department of Defense.⁸¹

The DoD has invested significantly in directed energy (DE) weapons, including on high-energy laser (HEL) and high-power microwave (HPM) systems capable of defeating sUAS. Lasers are cheap per shot, have large (so-called “unlimited”) magazines, and operate at the speed of light. However, they are technologically immature, expensive to build relative to other solutions, and offer limited

line-of-sight ranges. In 2014, the U.S. Navy fielded the first operational directed energy weapon, the Laser Weapon System (LaWS), aboard the USS *Ponce* (LPD-15). The ODIN and HELIOS systems are in development today. A variety of specifically anti-drone laser systems are now being developed as well, including the Athena and HELWS MRZR.

HPMs are another effector type. They are cheap per shot fired, technologically mature, and particularly effective against sUAS swarms with their potentially wide area of effect. However, future sUAS may harden against HPMs, although this would significantly raise their development costs and potentially lead to engineering difficulties.

The Army plans to equip the Leonidas as its primary HPM for indirect fires protection. Unlike other C-sUAS defenses that disable one drone at a time, Leonidas was engineered to kill swarms of Group 1 and 2 UAS, as demonstrated in several U.S. Army test events. The Army's Rapid Capabilities and Critical Technologies Office (RCCTO) recently awarded a \$66.1 million contract for Leonidas prototypes.⁸² Although HPMs have traditionally been based on larger platforms because of their large energy requirements, new technological developments are allowing for expanded basing options. The Leonidas Pod, for example, is a mobile, compact drone-based prototype that builds upon the ground-based system to offer relatively cheap, air-based C-sUAS.⁸³

Directed energy can be an effective C-sUAS tool. However, DE systems may encounter operational difficulties in complex and heavily congested environments, given the potential collateral damage to friendly forces and assets. Environmental factors such as poor weather or smoke in the atmosphere can also degrade their efficacy.⁸⁴ Furthermore, training requirements for directed energy platforms may be intensive. As one analyst explains, an operator's limited interaction time with an incoming UAS threat means that they must be well trained to deploy it effectively.⁸⁵

The last defeat modality is RF, through jamming or spoofing the drone's communications link. Global navigation satellite system (GNSS) spoofing—misleading its GPS—means that the operator can tell the drone that north is south, and west is east.⁸⁶ Jamming, conversely, means disrupting communications between the drone and its operator and is simpler to perform. Although RF-based defenses are powerful, operators must be aware of environmental effects potentially impacting nearby commercial or otherwise friendly aircraft.⁸⁷ RF-based defenses also do not affect autonomous or otherwise non-communicative UAS. Lastly, spoofing and jamming require defensive emissions, which may increase the risk that an adversary can geolocate defensive positions.

RF-based defenses have become increasingly popular over the last decade and operate as fixed, mounted, and handheld systems. In June 2020, six of eight systems selected to represent the JCO's interim C-sUAS capabilities utilized RF defeat: FS-LIDS, L-MADIS, CORIAN, NINJA, MEDUSA, and Dronebuster.⁸⁸ The Dronebuster is a handheld line-of-sight system weighing roughly four pounds, which allows for easy infantry and squad-level usage. Jamming capabilities also vary depending on the system; the Dronebuster Block 3 offers 45 minutes of jamming, whereas the updated Dronebuster SNA offers three hours of continuous jamming.⁸⁹

Table 10: Select C-sUAS Operations

Operator	Conflict	C-sUAS
Israel	Regular drone incursions from Hezbollah and Hamas	Iron Dome; Python-5; Skylord Griffon
Russia	Syrian civil war (2014–present)	Krasukha-4, Richag-AV radar and sonar jamming system; Moscow-1, Vitebsk
Russia	2014 Russian invasion of Crimea and 2022 Russian war on Ukraine	S-300; S-400; S-500; Pantsir-S systems
Ukraine	2014 Russian invasion of Crimea and 2022 Russian war on Ukraine	Gepard; Zu-23; small arms, National Advanced Surface-to-Air Missile Systems (NASAMS), IRIS-T; Aspide
Saudi Arabia	Intervention in the Yemeni civil war (2015–2022)	Indigenous and U.S. Patriot systems; Chinese Silent Hunter
Iraq	ISIS expansion in Iraq and Syria (2016–2018)	Small arms and machine guns

Source: CSIS Missile Defense Project.

A Diverse Solution Set

There are many different types of sensors, effectors, C2, and basing options for the C-sUAS mission. There is no single mix-and-match that serves as a universal solution to defeat sUAS threats. Rather, investment in a wide variety of sensors, effectors, and basing options is essential to ensure that the U.S. military is equipped to address the diverse set of threats posed by UAS. As JCO director Sean Gainey has explained, “There must be layers of systems to address the threat of UAS. It has to be a system of systems. It is a holistic approach.”⁹⁰

Sensors and effectors of various sorts have their own unique strengths and weaknesses. Kinetic effectors may be more reliable to take down any individual UAS threat—especially those that are bigger and faster. Non-kinetic effectors such as HPMs, on the other hand, can more effectively counter large UAS swarms.

Trade-offs likewise impact sensors. Active radar allows operators to detect threats at greater ranges but may give away their positions. Passive RF sensors allow operators to remain stealthy and are therefore the better option for dismounted, forward-deployed units. Yet passive RF sensors cannot detect pre-programmed UAS that do not communicate with their operator, which is becoming more prevalent on the battlefield. One-way attack drones, for example, have become common in Russian attacks against Ukrainian civil infrastructure. Overinvestment in one defense modality may leave defenders vulnerable in certain attack scenarios.

The need for diversity is likewise true in basing options. The right solution for a fixed site is different than that of a maneuver unit.⁹¹ A mobile defender may forsake having a range of effectors to remain small, light, and nimble so that they can shoot on the move. Fixed-site defenders, however, face adversaries that can plan sophisticated, large-scale attacks at various altitudes using a variety of missiles and UAS. Their defenses therefore require longer-range radars and effectors. Again, there is no one-size-fits-all material solution.

The Current Path

As senior leaders institutionalize the C-sUAS enterprise across the DOTMLPF, they must address critical gaps in training and personnel requirements.

U.S. efforts to develop effective C-sUAS operators and platforms can be loosely categorized in three stages: urgent need, refinement, and institutionalization. The United States is entering the third stage today, which will be the most difficult. It will require buy-in from the military services and clarity of roles throughout the defense establishment. The following sections define these stages, provide a historical overview of U.S. activities, and review what the United States must do to achieve institutionalization in the C-sUAS enterprise.

Table 11: Air and Missile Threat Matrix

	Target						
	Ballistic Missile	Cruise Missile	Rotary Wing	Fixed Wing	UAS Groups 1-3	UAS Groups 4 and 5	Rockets, Artillery, and Mortars
THAAD							
Patriot							
IFPC							
Stinger							
M-LIDS							
C-RAM							
DE, HPM, and HEL							

Source: U.S. Army.⁹²

Urgent Need

The U.S. response to C-sUAS has transpired in three stages. The first was urgent need. In 2016, ISIS captured large swaths of territory in both Iraq and Syria. They were among the first non-state actors to use small commercial quadcopters, which they employed effectively in battles against U.S.-supported Iraqi forces. There were few C-sUAS defenses in theater or readily deployable at the time. U.S. Central Command (CENTCOM) leadership issued an urgent requirement for defenses, prompting the DoD to quickly transfer a variety of commercial off-the-shelf C-sUAS platforms.

In 2016, the United States lacked cheaper, efficient effectors to use against cheap and plentiful sUAS. This lack was a consequence of wide divestment in Short-Range Air Defense (SHORAD) by the Army and Marine Corps in the 1990s and early 2000s. Both services were focused on the counterinsurgency mission in Afghanistan and Iraq and therefore chose to cut Air Defense Artillery (ADA) units in favor of more mission-critical maneuver forces. Military leadership believed that the U.S. Air Force would provide sufficient defensive counterair capabilities to maintain air superiority and protect ground forces.⁹³ Military leadership did not consider the threat of UAS and cruise missiles as viable, near-term threats to U.S. military operations. This trend was not uniquely American; most NATO nations also weakened their air defense capabilities over the last two decades.⁹⁴

Yet with the new threat clearly in sight, Congress has quickly committed funds to procure defenses. This step is highlighted by a significant surge in the DoD's FY 2017-FY 2019 procurement and research, development, testing, and evaluation spending for C-sUAS. While the DoD achieved an interim solution in months, it fully satisfied the C-sUAS Joint Urgent Operational Need (JUON) two years later in FY 2019. The initial JUON effort successfully committed defenses to provide an "interim standalone capability" to defend 89 CENTCOM sites against Groups 1 and 2 UAS.

Given the active threat to U.S. allied forces, the selection of defense systems was understandably fast paced. According to Barry J. Pike in 2018, then program executive officer for missiles and space, the C-sUAS budget was placed "in the same office as our Counter-Rocket, Artillery, and Mortar project because they do know how to go fast. . . . Within 60 days a requirement was generated and within another 60 days, we had materiel in theatre. . . . We fielded more than 270 different kinds of systems [for C-sUAS]."⁹⁵ A consequence of this quick delivery, however, was the minimal effort placed on the typical acquisition processes for programs of record and the DOTMLPF process. The massive quantity of C-sUAS platforms was deemed necessary at the time but would require the next stage in the C-sUAS response to consolidate these programs into a manageable portfolio.

Figure 15: Iranian-Made Kamikaze Drone



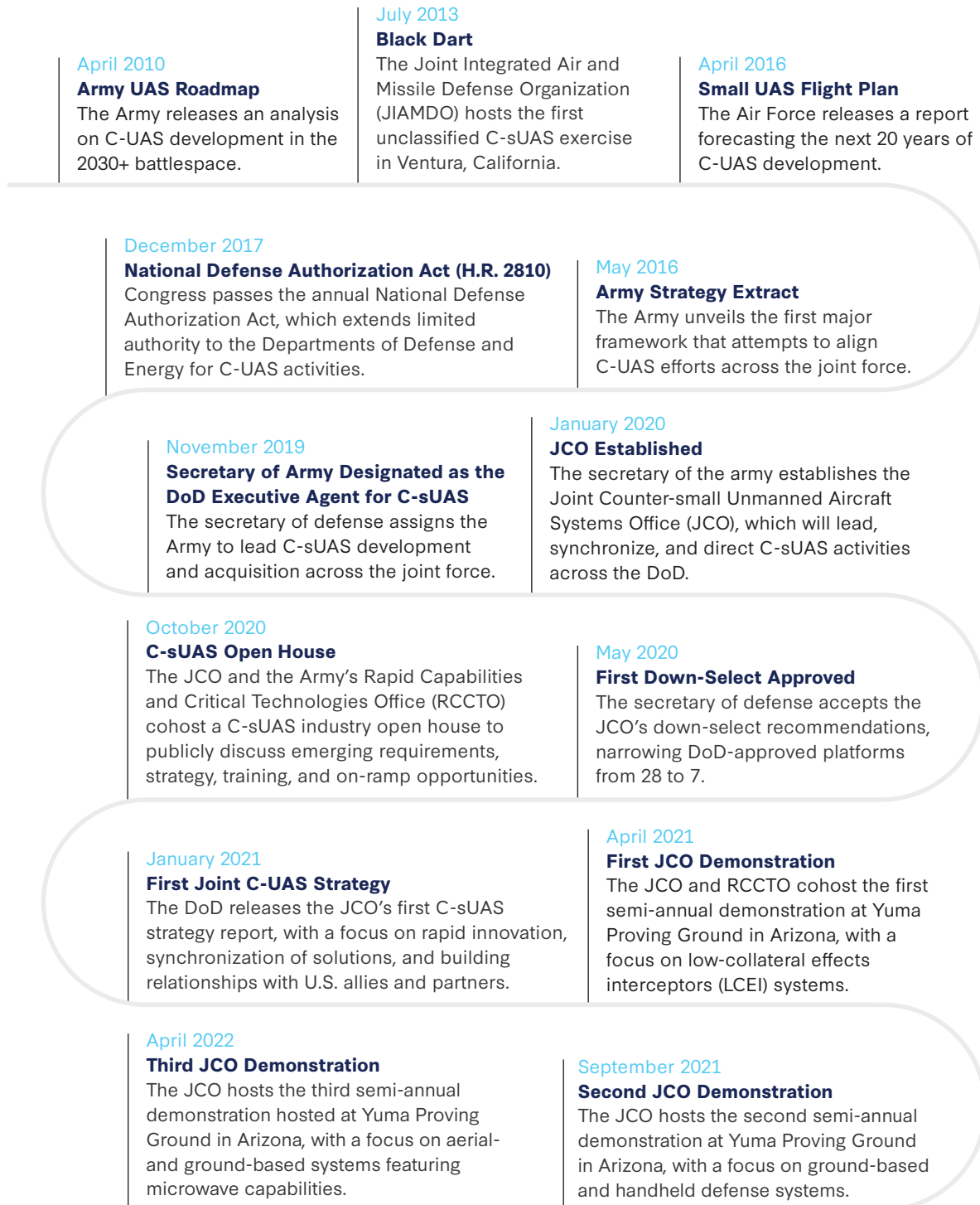
Remnants of Iranian-made kamikaze drone used by Houthi forces against Saudi Arabia.

Photo Credit: Jim Watson/AFP via Getty Images.

Refinement

The second stage in the U.S. response was one of refinement, during which the United States developed a more focused C-sUAS portfolio that was operationally effective and logistically sustainable. It included a diversity of sensors and effectors to cover the full threat spectrum. To fulfill this mission, in November 2019, the U.S. secretary of defense designated the Army as the lead service for C-sUAS; soon thereafter, the Army created the JCO to lead this effort. The JCO also helps the Army think through deployment strategies and align resources for C-sUAS. Recent budget justifications highlight this phase shift. The FY 2022 budget request noted the C-sUAS transition from a JUON to formal programming, with requirements specified under the Joint Requirements Oversight Council Memorandum 078-20. Also in FY 2022, the Army expanded the threat to include Group 3 UAS and designated a unique line-item number for C-sUAS. This move marked a symbolic emphasis on C-sUAS as a standalone program.

Figure 16: C-sUAS Milestones



Source: CSIS Missile Defense Project.

Institutionalization

The third and final stage is institutionalization, during which the United States must fill critical gaps across the DOTMLPF construct. The central question here is about how to apply air defense principles and institutionalize these capabilities to non-air defenders. The challenge is developing DOTMLPF solutions across the force to air defense and non-air defense units alike.

The military services will play a larger role in the institutionalization phase. Questions remain as to whether they will accept systems supported by the JCO or develop their own unique platforms more suited for their specific needs, as well as how such needs will be prioritized against other service needs. Major policy, strategy, budget, and programmatic decisions will be made that will carry enormous consequences for the field.⁹⁶

Table 12: DOTMLPF Plans and Potential Pitfalls

Element	Current Plans	Potential Pitfalls
Doctrine The principles that guide military forces as they pursue national security objectives. Often explains the most effective way of using military assets.	<ul style="list-style-type: none"> The JCO and services develop comprehensive, joint-service and service-specific doctrine for C-sUAS. 	<ul style="list-style-type: none"> Doctrine is not often shared, embraced, or applied appropriately in operations or materiel development. Doctrine does not clearly define that C-sUAS operations are a common combat task that all military specialties must contribute to and execute. Doctrine is trained in institutions, but its application in operations and materiel development remains challenging.
Organization How to build structures of people and equipment to fight (e.g., divisions, air wings, naval squadrons) and prepare to fight (e.g., acquisition offices).	<ul style="list-style-type: none"> The JCO serves as a central coordinator for C-sUAS development. The services distribute C-sUAS capabilities across the formations—not just to air defense personnel. 	<ul style="list-style-type: none"> The JCO does not have the authorities it requires to achieve its mission. The DoD's focus on consensus inhibits future transformation of the C-UAS enterprise to meet the threat.
Training How we prepare to fight tactically (e.g., training for individual service members, joint exercises, simulated war games).	<ul style="list-style-type: none"> The services train on established doctrine and share common Tactics, Techniques, and Procedures (TTPs) across the joint force. The services acknowledge and resource the Joint C-UAS Center of Excellence as the clearing house for C-sUAS TTPs, and relay operational lessons learned to update TTPs. 	<ul style="list-style-type: none"> The DoD does not invest the time, attention, and resources necessary for units to acquire an operational level of C-sUAS proficiency.
Materiel All of the stuff necessary to equip military forces so they can operate effectively.	<ul style="list-style-type: none"> The services balance C-sUAS development in light of fixed and mobile requirements. The services invest in a diverse sensor and shooter solution set. The services aim for C-sUAS integration and interoperability where possible and useful. 	<ul style="list-style-type: none"> C-sUAS acquisition authorities fail to invest adequately in forward-area maneuver requirements. C-sUAS acquisition authorities do not have the requirements, expertise, or time to satisfy integration or interoperability needs.

Leadership and Education

Leadership is influencing people by providing purpose, direction, and motivation, while operating to accomplish the mission and improve the organization.

Education is how we prepare our leaders to lead the fight.

- The services incorporate C-sUAS training across branch leader and soldier development and education programming.
- Leaders in non-air defense branches are unconvinced of their role in C-sUAS.

Personnel

The individuals required in either a military or civilian capacity to accomplish the assigned mission.

- The DoD encourages all units to learn how to combat Groups 1 and 2 UAS through both active and passive means, and is teaching air defenders TTPs for managing Group 3 threats.
- Uncertainty remains over C-sUAS roles and responsibilities between air defense and non-air defense specialists.

Facilities

The property, installations, and industrial plants that support our military forces.

- The Army is developing a permanent C-sUAS training installation in Fort Sill, Oklahoma.
- The Joint C-sUAS University's (JCU) location at Fort Sill dissuades Army maneuver personnel from attending.
- The JCU fails to include classes relevant for non-Army service members, so the other services do not attend.

Source: CSIS Missile Defense; DOTMLPF definitions from U.S. Department of Defense.⁹⁷

DOCTRINE

C-sUAS doctrine has improved significantly over the last decade. The DoD began developing C-sUAS tactics, techniques, and procedures over the late 2010s as the sUAS threat proliferated. The Army released three central documents during this period. The first was the 2016 Army Techniques Publication (ATP) 3-01.8, *Techniques for Combined Arms for Air Defense*. ATP 3-01.8 provides guidance on how combined arms forces can protect themselves from air attacks, including UAS threats.

The second central doctrine publication was the 2017 ATP 3-01.81, *Counter-Unmanned Aircraft System Techniques*. This report provides defense planning, training guidance, and regional threat preparations for sUAS threats. It highlights basic issues such as identifying specific UAS threats and potential responses based on the operational environment, enemy capabilities, and tactics. It also offers some specific combined arms unit training recommendations.⁹⁸

The third major doctrine publication was the 2020 Army Field Manual (FM) 3-01, *U.S. Army Air and Missile Defense Operations*. FM 3-01 incorporates details on the specific UAS threats and C-UAS techniques and offers some of the clearest guidance on countering sUAS to date. The report provides air defenders with established rules of engagement, along with guidance on the specific altitude, speed, and actions needed to determine whether a UAS is indeed a threat. Defensive measures are also explained down to the force level and divided by type, such as maneuver, aviation, special operating forces, field artillery, and intelligence (see Table 13). This clarified roles and responsibilities among the branches.

Table 13: Army C-sUAS Doctrine

C-sUAS Actions				
Maneuver Forces	Aviation Forces	Special Operating Forces	Field Artillery Forces	Intelligence Forces
<ul style="list-style-type: none"> • Passive defense • Engage in the air with organic small arms and crew-served weapons • Engage in the air with Stinger 	<ul style="list-style-type: none"> • Passive defense • Engage as targets of opportunity or in self-defense • Attack launch/airfield facilities and ground C2 station 	<ul style="list-style-type: none"> • Passive defense • Attack ground C2 station • Attack launch sites 	<ul style="list-style-type: none"> • Passive defense • Target C2 stations and launch sites • Support the air picture with data from artillery sensors • Engage in the air with small arms and crew-served weapons 	<ul style="list-style-type: none"> • Passive defense • Collect and analyze data regarding threat capabilities • Provide early warning • Provide targeting data for attack operations

Source: U.S. Army.⁹⁹

The primary concern is that doctrine is not often shared, embraced, or applied appropriately in operations or materiel development. One possible factor contributing to these issues is the lack of joint doctrine. Recognizing this underdevelopment, the 2018 Joint Publication (JP) 3-01, *Countering Air and Missile Threats*, called for more detailed UAS procedures on joint threat detection, identification, and engagement.¹⁰⁰ Since then, however, progress has been slow. For example, in its section on C-sUAS, the 2021 update to JP 3-30 *Joint Air Operations*, only noted the complexities of defeating sUAS and the need to distinguish between friendly and enemy sUAS.¹⁰¹ It failed to provide the kind of detail laid out in Army doctrine. Furthermore, now that the JCO has down-selected its primary C-sUAS sensors, C2, and effectors, a new joint publication could include specific C-sUAS platforms and operations to provide more clarity to service members.

The DoD must invest in future thinking to keep doctrine fresh as new challenges arise. This requires investing in internal and external leadership across the C-sUAS enterprise. The JCO—or another central authority—can coordinate and invest in this work and disseminate its findings. This may be done through joint military-academic dialogues, wargames, conflict simulations, and open-source intelligence collection and analysis on sUAS technologies and operations. The joint efforts of the military, academia, and defense industry can support the further evolution of doctrine at the pace required.

ORGANIZATION

The primary task of the military services is to organize, train, equip, and provide forces to the combatant commanders. In light of this goal, how will the services organize units or forces to perform the C-sUAS mission? Will the force structure for dedicated air defense forces within each service increase or will mission responsibility for the current forces merely expand? Will the services define a partitioning of mission responsibility between dedicated air defense forces and all other units and equip each accordingly?

Clearly, the C-sUAS mission mandates an increase in dedicated air defense force structure across the U.S. Army, Marine Corps, and Air Force, but the mission also requires an all-of-force approach

to defeating the UAS threat. Dedicated and non-dedicated air defense units must be prepared to perform active defense tasks and apply passive defense techniques to counter the UAS threat. The allocation of C-sUAS capability should align to mission responsibility, and the complexity of the materiel solutions, given the operational context they are applied in, should inform whether the capability requires a dedicated air defense crew or a non-dedicated operator. The concept of a CAFAD approach, across all services, should not be lost as the DoD organizes for this mission set.

Likewise, given the breadth and scope of the UAS challenge, the DoD should not lose sight of the fact that a single office to coordinate and guide development of C-sUAS capabilities might be of value. Since January 2020, the JCO has served as the central C-sUAS coordinator in the DoD, focused on establishing joint training, developing joint doctrine, and synchronizing joint materiel development. Because there is no one-size-fits-all for C-sUAS across the services, the JCO has promoted service-specific materiel and policy development while still working to reduce disparate and redundant investment, as is its mission. As a result, the DoD avoided investing in a larger number of platforms, greater redundancy among existing platforms, and increased maintenance, training, and logistics.

Yet the consensus model for C-sUAS may need to evolve over time. The current requirement for wide, cross-service consensus over C-sUAS investment could inhibit future transformation of the air defense enterprise to meet the threat.¹⁰² In the spectrum between development led by an all-powerful JCO on one end, and the Army and Marine Corps completely in charge of their own disparate plans on the other, today's acquisition enterprise may lean too far toward the latter camp. Congress and DoD leadership should reexamine JCO authorities and relation to service acquisition agencies to improve the requirements process and acquisition timelines. This could mean empowering the JCO with an authority requirement recognized by the Joint Capabilities Integration Development System (JCIDS) that is broad enough to be effective for immediate C-sUAS needs. This would need to be done, however, in coordination with service leadership to satisfy unique service requirements and avoid overlapping too much with other requirement generation bodies, such as the Army Futures Command Air and Missile Defense Cross-Functional Team (AMD CFT), which perhaps could focus more on longer-term C-sUAS requirements.

Outside of acquisition authorities, an empowered JCO might also lead C-sUAS coordination among the United States and its allies. The U.S. military spends significant resources to train and integrate its air defenses with allies and partners. These efforts have made joint operations safer and more effective in many theaters. In the C-sUAS arena, however, sales and joint partnerships are slow, and allies appear to rely mostly on RF sense and defeat platforms. Few NATO allies, for example, have invested in active defenses and instead appear to rely on passive defense, counterattacks, and general deterrence. As U.S. partners recognize the increasing sUAS threat—especially in light of Russia-Ukraine fighting today—the JCO can engage in dialogue and workshops to support U.S. exports, co-development, and joint training opportunities.

Figure 17: JCO Demonstration at Yuma Proving Ground



Industry and military officials attended the first JCO demonstration in April 2021 at Yuma Proving Ground, Arizona, where the focus was on low-collateral effects interceptors (LCEI) systems.

Photo Credit: Mark Schauer, U.S. Army.¹⁰³

TRAINING

Training is an urgent need across the joint force. The need for C-sUAS is on course to become ubiquitous for fixed and maneuver formations, necessitating a wide distribution and variety of training. As the JCO has affirmed, air defense specialists will continue to manage UAS threats for Groups 3 through 5, but the DoD should prepare all units to counter Groups 1 and 2. Commanders at all levels should incorporate C-sUAS in training exercises. Basic training must be simple enough to teach in a short window but comprehensive enough to cover this threat spectrum.

“You’re giving us \$10 billion worth of capabilities and \$10 of training.”

– U.S. Army master sergeant¹⁰⁴

There are currently four Joint Knowledge Online training modules that cover basic C-sUAS awareness, system familiarization, installation of C-sUAS activities, and C-sUAS tactics, techniques, and procedures.¹⁰⁵ These short, functional training courses are useful for familiarizing military personnel with sUAS threats and basic countermeasures.

A more comprehensive training program currently takes place at the C-sUAS Academy in Yuma, Arizona. It offers a two-week course, set to expand into a three-week class by FY 2025. The class is offered across the services and U.S. government, including Secret Service agents.¹⁰⁶ The Army also administers a “master trainer” course specifically for sUAS. Conducted at the Maneuver Center of Excellence in Fort Moore, Georgia, the training course certifies students with Group 1 UAS through a clear program of instruction which includes training on ground control stations, mission planning, simulations, orientation flights, and proficiency flight evaluations.¹⁰⁷ The upcoming Joint C-sUAS University (JCU) at the Fires Center of Excellence in Fort Sill, Oklahoma, discussed further in the “Facilities” subsection below, may consider building upon both training courses.

In FY 2024, the JCU will offer two courses—an operator and a planner course—each lasting two weeks. The operator course will provide service members with an additional skill identifier and consist of threat analysis, service specific engagement, and layered defense, with a capstone in detecting and defeating adversary drones. The planner course will consist of layered defense, coordination of airspace, joint strategic management, and C-sUAS planning and system integration, with a capstone in planning and executing a Course of Action (COA) to detect and defeat red air threats (single/swarming).

The DoD and JCO have prioritized training in recent years. Since April 2021, the JCO, RCCTO, and services have hosted industry demonstrations twice a year to “evaluate emerging technologies that close gaps, inform requirements, and promote innovation.”¹⁰⁸ This joins the service-focused exercises which have increasingly incorporated C-sUAS, as shown in the table below.

Table 14: Major U.S. C-sUAS Training and Development

Program	Description
Black Dart Exercises	This C-UAS exercise was classified until its first public event in 2013 and ran annually until 2019. In the initial exercises, the Pentagon noted the need for greater development of C-sUAS against Groups 1-3 given their growing global proliferation.
Hard Kill Challenge	This 2017 exercise was designed to evaluate technologies that can tackle UAS threats beyond 250 meters and with a “flyswatter approach.” C-sUAS testing results were mixed, with the Pentagon noting the resiliency of targets to deflect damage and the immaturity of most defenses.
Semi-annual JCO Demonstrations	The JCO hosts a semi-annual demonstration at Yuma Proving Ground, Arizona, to test various C-sUAS platforms. The first demonstration, held in April 2021, focused on LCEI systems. The second demonstration, held in September 2021, focused on ground-based and handheld defenses. The third demonstration, held in April 2022, focused on aerial- and ground-based systems employing microwave-based defenses.
Army’s High-Energy Laser System	The Army aims to develop two C-sUAS laser weapon systems with the ability to detect, track, and defeat Group 1 and 2 UAS threats. After conducting a capabilities gap analysis of HEL systems, RCCTO accelerated the preexisting program from FY23 to FY22 in October 2021.
Army’s High-Power Microwave System	The Army aims to deliver a fielded HPM capability to protect the force against Group 1 and 2 swarms. RCCTO began accelerating the IFPC-HPM program in FY23.
NATO’s C-UAS Technical Interoperability Exercise	This yearly exercise, which began in 2021, is led by NATO’s Communications and Information Agency in the Netherlands. TIE 2021 featured 70+ systems including sensors, counter-drone equipment, C2 systems, and drone threats. Tie 2022 focused on airspace security challenges, particularly AI/ML-based C-UAS technologies.

Navy C-UAS Training

The Pacific Target Marine Operations deployed sUAS to provide familiarization and threat training at Point Mugu in January 2022. This training focused on C-sUAS capabilities against Group 1 drones, with the key security concern being ISR.

Red Sands Integrated Experimentation Center

In a December 2022 press briefing, CENTCOM presented plans for a joint training program at the Red Sands Integrated Experimentation “Center,” with the goal of testing C-UAS technology. The center will focus on developing the Middle East’s air defenses. While initially proposed as a specific training ground in Saudi Arabia, it has been confirmed that Red Sands will shift locations, aligning with project-specific necessities.

Joint C-UAS University at Fort Sill in Oklahoma

The Army’s Fires Center of Excellence is creating the Joint C-UAS University in Fort Sill, Oklahoma, with initial operation beginning in the first quarter of FY 2024. The center is set to standardize practices and create C-UAS subject experts for joint training. The training program will include a common program of instruction, joint TTPs, and updated doctrine.

Source: CSIS Missile Defense Project.

Lessons from the field—especially in Ukraine—highlight how quickly the sUAS threat and tactics are evolving in real time. The lack of designated training ranges that have standing C-sUAS authorities to operate within CONUS airspace hinders the ability of DoD to train on new equipment and stress test the validity of new TTPs. Resources such as the Joint C-UAS Center of Excellence and the Joint C-UAS University (JCU) are being stood up to address such gaps in training knowledge across the joint force and act as a clearing house for C-sUAS TTPs. Ultimately, range location issues and reduced live training opportunities will hinder efforts to build readiness, particularly for directed energy systems.

Matériel

C-sUAS matériel development was addressed in Chapter 2 of this report. In short, matériel development should feature a diverse solution set informed by formation requirements for fixed or mobile defenses. Today’s platforms focus primarily on fixed requirements, as requested by CENTCOM and available at the time. Yet as the maneuver force sees the need for C-sUAS across regions, the DoD will need to shift focus toward mobile and maneuver capabilities.

Leadership and Education

Professional leadership development—from squad leaders to flag officers—must be a priority to ensure doctrine and training are effectively implemented. C-sUAS leaders across air defense, maneuver, support, and sustainment teams will help drive operational planning and training across the force and at the various echelons they lead. These leaders can also help identify and respond to sUAS development trends and adversary capabilities and construct new TTPs in line with emerging technologies. The DoD is building C-sUAS leaders through the several training programs listed above in the “Training” section.

Personnel

The C-sUAS mission must be shared across air defense and all other combat, combat support, and combat service support activities. The high demand and low density of air defense formations requires that air defenders and non-specialists work together as part of a CAFAD approach. The central question today, however, is the specific division of labor among the air defense and non-air defense units. Table 15 below lays out three models to illustrate the terms of this debate. On one end is the “Specialized” model, in which the C-sUAS mission is largely taken on by air defenders. On the other end, the “Universal” model posits a framework in which all units are trained for C-sUAS. The “Specialized” and “Universal” models are extremes for illustrative purposes—no one advocates for these purist frameworks. U.S. defense officials are developing an appropriate middle path, labeled

here as “Hybrid,” which will incorporate elements from both sides. The degree of specialization versus universalization, however, remains to be determined.

Table 15: C-sUAS Operator Frameworks

Model	Features	Strengths	Weaknesses
Specialized	<ul style="list-style-type: none"> Develop a specialized C-sUAS Military Occupational Specialty (MOS). Increase recruitment for ADA, and integrate those personnel back into the maneuver forces. 	<ul style="list-style-type: none"> Training is focused and extensive, allowing defenses to be tailored to threats and updated more frequently. 	<ul style="list-style-type: none"> More requirements for training, personnel, cost. Potentially slower response time because only authorized C-UAS operators can counter threats. Concentrated training means centralized points of failure.
Hybrid	<ul style="list-style-type: none"> Keep the divide between “asset” and “self” defenses, with air defenders focused on the former and everyone familiar with the latter. Develop C-sUAS specialists within and outside of the air defense branch. 	<ul style="list-style-type: none"> Provides more robust capability to the most critical assets. Provides some level of capability to all units. 	<ul style="list-style-type: none"> Requires investment in more equipment and dedication of training time to equip non-ADA soldiers. Non-ADA units may not commit time and personnel to master the C-UAS capabilities.
Universal	<ul style="list-style-type: none"> All units are trained for C-sUAS of all types. 	<ul style="list-style-type: none"> Distributed training means fewer points of failure in combat. 	<ul style="list-style-type: none"> Training is less effective or costs more to teach a larger population.

Source: CSIS Missile Defense Project.

Under the hybrid model, C-sUAS planners have borrowed the distinction between “area” and “point” defense whereby air defenders manage larger systems such as high-energy lasers and long-range kinetic interceptors for “area” defense, while other forces use “point” defenses such as guns, nets, and handheld platforms. Maneuver and forward-deployed forces should be able to detect and classify Groups 1 and 2 and, if unable to intercept themselves, at least “relay alert information on locations, altitudes, and time” critical to ground force protection and the possible defeat of enemy UAS.¹⁰⁹ The JCO’s investments suggest an emphasis on CAFAD. Handheld jammers, targeting enhancers, the smart shooter, and other smaller platforms have left this pathway open for the joint force across all units.

The hybrid model posits that the C-sUAS mission in non-ADA units is a force protection task, akin to chemical defense operations. All personnel have a responsibility to perform self-protection chemical defense tasks, and select personnel are trained to employ chemical defense equipment, such as chemical detection kits or alarms. Under the C-sUAS construct, all personnel must be able to engage an sUAS with their assigned or unit organic weapons, and select personnel will be trained to employ C-sUAS weapons.

Questions over specific platforms, specializations, and authorities, however, are still up for debate. Should the infantry operate M-LIDS as a divisional level asset, or should this type of platform be forward deployed at the company level? How much training does a soldier need to fire a Coyote missile? Should the Army significantly expand SHORAD units as the Marine Corps has done by tripling the size of the Low Altitude Air Defense Marines community?¹¹⁰ And how can ground forces deconflict with the Air Force and allied air forces in a timely, effective manner? The DoD needs to answer these questions to

fully institutionalize the C-sUAS enterprise. Doing so will allow staff to better understand how C-sUAS formations will work across services and branches, as well as how to plan against sUAS threats.

Facilities

The Army's plans for facility development are underway. Previous C-sUAS training operations were conducted out of Yuma Proving Ground and lasted roughly two weeks. Despite this training and other branch-specific programs, the JCO found a lack of institutionalized C-UAS training, with one senior Air Force officer noting, "There are currently no joint linkages or commonality to counter UAS training across the department. . . . The average soldier, airman, or Marine lacks adequate counter UAS training."¹¹¹ To improve the military's C-sUAS capabilities and create a permanent training installation, the Fires Center of Excellence in Fort Sill, Oklahoma, is building a Joint C-sUAS University (JCU), which is scheduled to reach initial operation in the first quarter of FY 2024.¹¹² The academy will provide a common core program of instruction, joint TTPs, and updated doctrine.¹¹³ The center will also provide the C-sUAS community with additional space and equipment to conduct research, test, and train.

The JCU's location at Fort Sill is understandable but suggests a larger role for air defenders over the maneuver force for C-sUAS training. Will this truly be a joint center for all branches, or will the Maneuver Center of Excellence (MCoE) at Fort Moore, Georgia, develop its own C-sUAS doctrine to inform mobile and maneuver C-sUAS requirements? Furthermore, while most C-sUAS specialists will likely be Army soldiers, the Army-centric location may also discourage Marines from joining. These concerns can be managed as long as the JCU recruits from across the services and branches upon its opening in FY 2024.

Figure 18: Preparing RQ-7B Shadow for Flight



Oklahoma Army National Guard soldiers and contractors prepare an RQ-7B Shadow for flight at Fort Sill.

Source: U.S. Army.¹¹⁴

Conclusion

The sUAS threat is here to stay. These systems offer multi-mission capabilities, at low cost, and with minimal signatures. They are widely available through commercial industry and their utility has been demonstrated in numerous conflicts around the world, from the Russian invasion of Ukraine, to Azerbaijan and Armenia's conflict over Nagorno-Karabakh, to the Yemen civil war. Given these factors, sUAS technology will continue to evolve and proliferate.

As such, C-sUAS has become a critical part of modern air defense. That criticality, however, does not mean that the joint force is ready for the challenge. Today's air and missile defense systems and structures were not designed to counter numerous, low-flying, small uncrewed systems. sUAS exploit gaps in sensor coverage and cost asymmetries against expensive interceptors. The belief that aerial threats would be countered by U.S. air forces or the ballistic missile defense force may have been true at one point, but drone technology evolved far faster than most thought possible. The U.S. divestment of SHORAD left the DoD without tools and personnel that may have more easily adapted to the sUAS threat, although the proliferation and sophistication seen today calls for more than the SHORAD of yesteryear.

Fortunately, there is a diverse mix of sensors, effectors, and C2 systems that can detect, track, identify, and defeat sUAS. The DoD is investing in a variety of kinetic, electronic, and RF-based defenses to counter sUAS threats. These tools have their respective strengths and weaknesses affecting such factors as survivability, range, magazine capacity, combat identification, and total defended area. Defense budgets here are limited, but the JCO has down-selected across a wide array of C-sUAS platforms to improve economies of scale in production, logistics, and training.

The institutionalization of C-sUAS will require developments across doctrine, organization, training, materiel, leadership and education, personnel, and facilities. Capability development remains necessary for the long term, but as the JCO has emphasized, the urgent need today is for training and capacity. New doctrine should specify the division of labor between air defense and non-air defense specialists, as well as the specific sensors, C2, and effectors that they can operate. C-sUAS leaders will need to tackle these and various other challenges, with their decisions today shaping the field for years to come.

Authors

Shaan Shaikh is the deputy director of the CSIS Missile Defense Project, where he focuses on missile proliferation, uncrewed aerial systems, air defense, and non-state actors. He is also managing editor of the CSIS website *Missile Threat*, an online clearinghouse for information and analysis on missile and missile defense systems. Prior to joining CSIS, he worked at the U.S. Department of Defense and The Syria Institute. He is currently a graduate student at the Johns Hopkins School of Advanced International Studies and holds a BA in international relations and Arabic from Tufts University.

Tom Karako is a senior fellow with the International Security Program and the director of the Missile Defense Project at CSIS, where he arrived in 2014. His research focuses on national security, missile defense, nuclear deterrence, and public law. In 2010-2011, he was an American Political Science Association congressional fellow, working with the professional staff of the House Armed Services Committee and the Subcommittee on Strategic Forces on U.S. strategic forces policy, nonproliferation, and NATO. Dr. Karako is also currently a fellow with the Institute for Politics and Strategy of Carnegie Mellon University. He received his PhD from Claremont Graduate University and his BA from the University of Dallas.

Michelle McLoughlin is a former intern with the CSIS Missile Defense Project. She is currently a graduate student at American University's School of International Service and holds a BA in international relations from the University of San Diego.

Endnotes

INTRODUCTION

- 1 Kelley Saylor, *A World of Proliferated Drones: A Technology Primer* (Washington, DC: Center for a New American Security, June 2015), <https://www.cnas.org/publications/reports/a-world-of-proliferated-drones-a-technology-primer>; and Dan Gettinger, *The Drone Databook* (Annandale-on-Hudson, NY: Center for the Study of the Drone, Bard College, September 2019), <https://dronecenter.bard.edu/files/2019/10/CSD-Drone-Databook-Web.pdf>.
- 2 Arthur Holland Michel, *Counter-Drone Systems* (Annandale-on-Hudson, NY: Center for the Study of the Drone, Bard College, December 2019), 2nd ed., <https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf>.
- 3 U.S. Department of Defense, *National Defense Strategy of the United States of America* (Washington, DC: October 2022), 8, 12, <https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF>.
- 4 Kettering Bug, U.S. Army, <https://commons.wikimedia.org/wiki/File:Kettering-bug-1.jpeg>; MQ-1 Predator, U.S. Air Force Photo by Tech Sgt. Effrain Lopez, <https://www.dvidshub.net/image/509547/mq-1-predator-flight>; and DJI Mini 2, Robert Myers via Wikimedia Commons (licensed under CC-BY-SA 3.0 AU), [https://commons.wikimedia.org/wiki/File:DJI_Mini_2_in_flight_\(cropped\).jpg](https://commons.wikimedia.org/wiki/File:DJI_Mini_2_in_flight_(cropped).jpg), licensed under CC-BY-SA 3.0 AU. In accordance with the Creative Commons license, Figure 1 is likewise licensed under CC-BY-SA 3.0.
- 5 Joint Chiefs of Staff, *Joint Publication 3-01: Countering Air and Missile Threats* (JP 3-01) (Washington, DC: Joint Chiefs of Staff, May 2018), https://irp.fas.org/doddir/dod/jp3_01.pdf.

CHAPTER 1: THE SUAS THREAT

- 6 Andrew E. Kramer, “Missile Barrage Staggers Ukraine’s Air Defenses,” *New York Times*, December 29, 2022, <https://www.nytimes.com/2022/12/29/world/europe/russia-strikes-ukraine.html>.

- 7 Kathleen Magramo et al., “December 29, 2022 Russia-Ukraine news,” CNN, December 30, 2022, <https://www.cnn.com/europe/live-news/russia-ukraine-war-news-12-29-22/index.html>.
- 8 Ian Williams, *Putin’s Missile War* (Washington DC: CSIS, 2023), 11-12, 43-44, <https://www.csis.org/analysis/putins-missile-war>.
- 9 Courtney Kube and Mosheh Gains, “Drone attacks on American bases injured two dozen U.S. military personnel,” NBC News, October 24, 2023, <https://www.nbcnews.com/politics/national-security/drone-attacks-american-bases-injured-two-dozen-us-military-personnel-rcna121961>.
- 10 Gili Cohen, “Israel Unsuccessfully Tries to Intercept Drone That Breached Its Airspace,” *Haaretz*, July 17, 2016, <https://www.haaretz.com/israel-news/2016-07-17/ty-article/israel-tries-fails-to-intercept-drone-over-that-breached-its-airspace/0000017f-dc2c-df62-a9ff-dcfffdb40000>.
- 11 David Hambling, “New Saudi Missile Order Reveals The High Cost Of Asymmetric Drone War,” *Forbes*, November 11, 2021, <https://www.forbes.com/sites/davidhambling/2021/11/11/new-missile-order-reveals-true-cost-of-asymmetric-drone-war/?sh=28f22ae816f2>.
- 12 Dave Ehredt, “NATO - Joint Air Power Competence Centre,” NATO, Joint Air Power Competence Center, 2010, http://www.dcabr.org.br/download/eventos/eventos-realizados/2010/seminario-vant-27-10-2010/cd-uvs-yearbook/pdf/P061-062_NATO_Dave-Ehredt.pdf.
- 13 Department of the Army, *Counter Unmanned Aerial System (C-UAS)*, ATP 3-01.81 (Washington, DC: Department of Defense, August 2023), 1-3, <https://irp.fas.org/doddir/army/atp3-01-81.pdf>. Images: DJI Phantom 3, Zeynel Cebeci via Wikimedia Commons (licensed under CC BY 3.0 DEED), June 9, 2013, https://commons.wikimedia.org/wiki/File:Quadcopter_03_trimming.JPG; Orlan-10, Russian Ministry of Defence via Wikimedia Commons (licensed under CC BY 4.0 DEED), April 23, 2014, <https://commons.wikimedia.org/wiki/File:Orlan-10.jpg>; Forpost, Russian Ministry of Defense, https://function.mil.ru/news_page/country/more.htm?id=12292395@egNews; Wing Loong (Yilong 1), Wikimedia Commons (licensed under CC-BY-SA 4.0), July 22, 2017, [https://commons.wikimedia.org/wiki/File:Wing_loong_MAKS2017_\(cropped\).jpg](https://commons.wikimedia.org/wiki/File:Wing_loong_MAKS2017_(cropped).jpg); and BZK-005, Japanese Ministry of Defense via Wikimedia Commons (licensed under CC BY 4.0 DEED), January 30, 2013, https://commons.wikimedia.org/wiki/File:PLA_Drone_BZK-005_2023-08-28.jpg. In accordance with the Creative Commons license, Table 1 is likewise licensed under CC-BY-SA 4.0.
- 14 “NATO UAS Classification,” in Róbert Szabolcsi, “Beyond Training Minimums - A New Concept of the UAV Operator Training Program,” International Conference Knowledge-Based Organization 22, no. 3 (July 2016), doi:10.1515/kbo-2016-0096; Black Widow, Vulcan UAS, accessed July 18, 2023, reprinted with permission, <https://www.aeroexpo.online/prod/vulcan-uav/product-181301-72985.html>; Skylark 3, Elbit Systems, accessed July 18, 2023, reprinted with permission, <https://elbitsystems.com/pr-new/elbit-systems-to-showcase-hybrid-propulsion-small-tactical-uas-at-singapore-airshow-2022/>; Scan Eagle, U.S. Navy via Wikimedia Commons, October 15, 2016, [https://commons.wikimedia.org/wiki/File:US_Navy_1005268-N-RC844-159_A_Scan_Eagle_Unmanned_Aerial_Vehicle_\(UAV\).jpg](https://commons.wikimedia.org/wiki/File:US_Navy_1005268-N-RC844-159_A_Scan_Eagle_Unmanned_Aerial_Vehicle_(UAV).jpg); Hermes 450, Elbit Systems, reprinted with permission; Heron 1, U.S. Air Force by Reyonaldo Ramon via Wikimedia Commons, August 13, 2003, [https://commons.wikimedia.org/wiki/File:IAI_Heron\(framed\).jpg](https://commons.wikimedia.org/wiki/File:IAI_Heron(framed).jpg); RQ-4 Global Hawk, U.S. Air Force photo by Bobbi Zapka via Wikimedia Commons, March 1, 2007, https://commons.wikimedia.org/wiki/File:Global_Hawk_1.jpg; and MQ-9 Reaper, U.S. Air Force by Airman 1st Class William Rio Rosado, July 15, 2019, <https://www.af.mil/News/Photos/igphoto/2002864740/mediaid/5461089/>.
- 15 Todd Harrison, “Rethinking the Role of Remotely Crewed Systems in the Future Force,” CSIS, *CSIS Briefs*, March 3, 2021, <https://www.csis.org/analysis/rethinking-role-remotely-crewed-systems-future-force>.
- 16 For more on UAS shootdown risks compared to those of inhabited aircraft, see Erik Lin-Greenberg, “Wargame of Drones: Remotely Piloted Aircraft and Crisis Escalation,” *Journal of Conflict Resolution*, 66

no. 10 (2022), doi:10.1177/00220027221106960.

- 17 Christina Mackenzie, “After Ukraine, French air force zeroes in on anti-drone strategy: Air chief,” *Breaking Defense*, February 10, 2023, <https://breakingdefense.com/2023/02/after-ukraine-french-air-force-zeroes-in-on-anti-drone-strategy-air-chief/>.
- 18 Jack Watling and Nick Reynolds, *Meatgrinder: Russian Tactics in the Second Year of Its Invasion of Ukraine* (London: Royal United Services Institute, May 2023), <https://rusi.org/explore-our-research/publications/special-resources/meatgrinder-russian-tactics-second-year-its-invasion-ukraine>.
- 19 Jack Detsch, “‘It’s Not Afghanistan’: Ukrainian Pilots Push Back on U.S.-Provided Drones,” *Foreign Policy*, June 21, 2022, <https://foreignpolicy.com/2022/06/21/ukraine-us-drones-pushback/>.
- 20 Ian Williams, *Putin’s Missile War: Russia’s Strike Campaign in Ukraine* (Washington, DC: CSIS, May 2023), <https://www.csis.org/analysis/putins-missile-war>.
- 21 Benjamin Jensen and Matthew Strohmeier, “The Changing Character of Combined Arms,” *War on the Rocks*, May 23, 2022, <https://warontherocks.com/2022/05/the-changing-character-of-combined-arms/>.
- 22 Ian Williams, “How drone attacks reveal fixable flaws with American air defenses,” *The Hill*, September 24, 2019, <https://thehill.com/opinion/national-security/462661-how-drone-attacks-reveal-fixable-flaws-with-american-air-defenses/>.
- 23 Yun Li, “Saudi oil production cut by 50% after drones attack crude facilities,” *CNBC*, September 14, 2019, <https://www.cnn.com/2019/09/14/saudi-arabia-is-shutting-down-half-of-its-oil-production-after-drone-attack-wsj-says.html>.
- 24 Farzin Nadimi, “Iranian Drones to Russia: Capabilities and Limitations,” *Washington Institute for Near East Policy*, August 1, 2022, <https://www.washingtoninstitute.org/policy-analysis/iranian-drones-russia-capabilities-and-limitations>.
- 25 Patricia Laya, “Venezuela Arrests Six After Maduro Escapes Explosive Drone Attack,” *Bloomberg*, August 4, 2018, <https://www.bloomberg.com/news/articles/2018-08-04/maduro-led-away-from-military-parade-after-explosion-heard>.
- 26 Nick Waters, “Houthi Use Armed Drone to Target Yemeni Army Top Brass,” *Bellingcat*, January 20, 2019, <https://www.bellingcat.com/news/mena/2019/01/10/houthi-usearmed-drone-to-target-yemeni-army-top-brass/>.
- 27 Qassim Abdul-Zahra, “Iraqi prime minister survives assassination bid with drones,” *Associated Press*, November 7, 2021, <https://apnews.com/article/middle-east-fires-iraq-baghdad-embassies-4069e75a45ee9b4eaa5e93648fa15211>.
- 28 Michael S. Schmidt and Eric Schmitt, “Pentagon Confronts a New Threat From ISIS: Exploding Drones,” *New York Times*, October 11, 2016, <https://www.nytimes.com/2016/10/12/world/middleeast/iraq-drones-isis.html>.
- 29 Joby Warrick, “Use of weaponized drones by ISIS spurs terrorism fears,” *Washington Post*, February 21, 2017, https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html.
- 30 Shaan Shaikh and Wes Rumbaugh, “The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense,” CSIS, *Critical Questions*, December 8, 2020, <https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense>.
- 31 Shaan Shaikh, “Iranian Missiles in Iraq,” CSIS, *CSIS Briefs*, December 11, 2019, <https://www.csis.org/analysis/iranian-missiles-iraq>.

- 32 Rick Broida, “Get a DJI Phantom 1 quad-copter for \$379,” CNET, January 8, 2015, <https://www.cnet.com/tech/computing/get-a-dji-phantom-1-quad-copter-for-379/>.
- 33 “Phantom,” DJI, December 7, 2013, <https://web.archive.org/web/20131207044205/http://www.dji.com/tech-spec/phantom-sepc/>.
- 34 Bill Canis, *Unmanned Aircraft Systems (UAS): Commercial Outlook for a New Industry*, CRS Report no. R44192 (Washington, DC: Congressional Research Service, September 2015), <https://crsreports.congress.gov/product/pdf/R/R44192/4>.
- 35 “Commercial sUAS (Drone) Market Trends, Stats, Forecasts, Products, Services, Industries, and Regions,” ABIresearch, July 13, 2022, <https://www.abiresearch.com/blogs/2022/07/13/commercial-suas-drone-market-trends-stats-forecasts-products-services-industries-and-regions/>.
- 36 Allied Market Research, *Commercial Drones Market: Global Opportunity Analysis and Industry Forecast 2021-2030* (Portland, OR: Allied Market Research, 2022), <https://www.alliedmarketresearch.com/commercial-drone-market>.
- 37 “Mavic 3 - Specs,” DJI Official, <https://www.dji.com/mavic-3/specs>; “Phantom 1 - Product Information,” DJI Official, <https://www.dji.com/phantom/info>. Figures in then-year USD.
- 38 Canis, *Unmanned Aircraft Systems*, 4.
- 39 Nora Manthey, “LG Chem proves Li-sulfur battery stable in high flight,” Electrive, September 11, 2020, <https://www.electrive.com/2020/09/11/lg-chem-proves-li-sulfur-battery-stable-in-high-flight/>.
- 40 “Technology Quarterly Taking Flight,” *The Economist*, June 8, 2017, <https://www.economist.com/technology-quarterly/2017-06-08/civilian-drones>.
- 41 “Military Drones Market to Garner \$34.34 Billion by 2031: Allied Market Research,” Allied Market Research, August 17, 2022, <https://www.globenewswire.com/en/news-release/2022/08/17/2499646/0/en/Military-Drones-Market-to-Garner-34-34-Billion-by-2031-Allied-Market-Research.html>; and Jeremiah Gertler, *U.S. Unmanned Aerial Systems*, CRS Report no. R42136 (Washington, DC: Congressional Research Service, January 2012), <https://sgp.fas.org/crs/natsec/R42136.pdf>.
- 42 Dan Gettinger, “Drone Databook Update: March 2020,” Center for the Study of the Drone, Bard College, March 2020, <https://dronecenter.bard.edu/projects/drone-proliferation/drone-databook-update-march-2020/>.
- 43 Gettinger, *Drone Databook*, 2019, ix.
- 44 David Hylton, “75th Ranger Regiment Receives Short Range Reconnaissance System,” U.S. Army, December 1, 2022, https://www.army.mil/article/262425/75th_ranger_regiment_receives_short_range_reconnaissance_system; and Kelsey D. Atherton, “The Army skips off-the-shelf drones for a new custom quadcopter,” Popular Science, December 12, 2022, <https://www.popsoci.com/technology/army-drone-military-use/>.
- 45 “Joint Declaration for the Export and Subsequent Use of Armed or Strike-Enabled Unmanned Aerial Vehicles (UAVs),” U.S. State Department, Bureau of Political-Military Affairs, October 16, 2017, <https://2017-2021.state.gov/joint-declaration-for-the-export-and-subsequent-use-of-armed-or-strike-enabled-unmanned-aerial-vehicles-uavs/index.html>.
- 46 Erik Lin-Greenberg, “New Declaration on UAV Exports Unlikely to Reduce Drone Proliferation,” Lawfare, November 20, 2016, <https://www.lawfareblog.com/new-declaration-uav-exports-unlikely-reduce-drone-proliferation>.
- 47 Don Rassler, *The Islamic State and Drones: Supply, Scale, and Future Threats* (West Point, NY: Combating

Terrorism Center at West Point, July 2018), <https://ctc.westpoint.edu/wp-content/uploads/2018/07/Islamic-State-and-Drones-Release-Version.pdf>.

- 48 “Evolution of UAVs employed by Houthi forces in Yemen,” Conflict Armament Research, April 6, 2021, <https://storymaps.arcgis.com/stories/46283842630243379f0504ece90a821f>.
- 49 “Counter-Small Unmanned Aircraft Systems Strategy,” U.S. Department of Defense, 6, <https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF>.
- 50 Gregory Allen, “DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread,” CSIS, *Commentary*, June 6, 2022, <https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread>.
- 51 Andrew Eversden, “Army must start ‘leaning’ on kinetic options for counter-drone as autonomous UAS proliferate,” Breaking Defense, August 11, 2022, <https://breakingdefense.com/2022/08/army-must-start-leaning-on-kinetic-options-for-counter-drone-as-autonomous-uas-proliferate/>.
- 52 David Hambling, “This Record-Breaking Shanghai Drone Display Is A Show Of Technological Strength,” Forbes, April 6, 2021, <https://www.forbes.com/sites/davidhambling/2021/04/06/why-this-record-breaking-drone-display-in-shanghai-is-a-show-of-technological-strength/?sh=4c2cb5822d53>.
- 53 Eversden, “Army must start ‘leaning’ on kinetic options for counter-drone.”
- 54 Ibid.

CHAPTER 2: DETECTING AND DEFEATING SUAS

- 55 Ibid.; and National Urban Security Technology Laboratory, *Counter-Unmanned Aerial Systems Technology Guide* (Washington, DC: Department of Homeland Security, September 2019), 20, https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.
- 56 Higher frequency radar such as Ku-Band is preferred for relatively small aperture that enables a small platform, such as the M-SHORAD vehicle, to mount a system that provides excellent track capability. However, higher frequencies are ultimately limited in longer-range detection performance given its effective radiated power versus physically larger systems.
- 57 Ibid.
- 58 National Urban Security Technology Laboratory, *Counter-Unmanned Aerial Systems Technology Guide*, 18.
- 59 “Counter Rocket, Artillery, and Mortar (C-RAM),” DRS RADA Technologies, <https://www.drsrcada.com/missions/c-ram>. Reprinted with permission.
- 60 “Army announces selection of interim C-sUAS systems,” U.S. Army, June 25, 2020, https://www.army.mil/article/236713/army_announces_selection_of_interim_c_suas_systems.
- 61 “Counter-Small Unmanned Aerial Systems (UAS) Systems,” U.S. Army - Director, Operational Test and Evaluation, January 2021, <https://www.dote.osd.mil/Portals/97/pub/reports/FY2020/army/2020csuas.pdf>.
- 62 Loz Blain, “World’s first laser-controlled drone easily evades countermeasures,” New Atlas, July 21, 2022, <https://newatlas.com/drones/laser-control-drone-qinetiq/>.
- 63 National Urban Security Technology Laboratory, *Counter-Unmanned Aerial Systems Technology Guide* (Washington, DC: Department of Homeland Security, September 2019), 20, https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf; FS-LIDS, SRC Technologies, accessed July 18, 2023, reprinted with permission, <https://www.srcinc.com/news-and-events/>

- press/2020/20201203-src-technology-chosen-for-dod-fixed-site-counter-uas-solution.html; LPWS, U.S. Army photo by Sgt. Jarred Woods, March 1, 2014, <https://www.dvidshub.net/image/1182163/protecting-force>; M-LIDS, U.S. Army photo by Spc. Damian Mioduszcwski, January 22, 2022, <https://www.dvidshub.net/image/7028562/m-lids>; Discovair, Squarehead Technology, accessed July 18, 2023, reprinted with permission, <https://www.sqhead.com/defense>; EnforceAir, D-Fend Solutions, reprinted with permission.
- 64 Joint Chiefs of Staff, *Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms* (Washington, DC: Department of Defense, updated February 2016), 40, https://irp.fas.org/doddir/dod/jp1_02.pdf.
 - 65 Joint Chiefs of Staff, *Joint Publication 3-01*, 176, III-9.
 - 66 U.S. Army, *Weapons Systems Handbook: 2020-2021* (Washington, DC: U.S. Army, May 2020), 176, https://www.army.mil/e2/downloads/rv7/2020-2021_Weapon_Systems_Handbook.pdf.
 - 67 Kelsey Reichmann, “FAAD C2 Basis for DoD C-sUAS Effort,” *Defense Daily*, January 8, 2021, <https://www.defensedaily.com/faad-c2-basis-dod-c-suas-effort/unmanned-systems/>.
 - 68 Ibid.
 - 69 “Forward Area Air Defense Command and Control (FAAD C2),” U.S. Army Acquisition Support Center, Last updated 2023, <https://asc.army.mil/web/portfolio-item/anmpq-64-sentinel-2/>.
 - 70 Meghan E. Hall, “Innovation Draws International Interest,” U.S. Army Acquisition Support Center, December 20, 2021, <https://asc.army.mil/web/news-innovation-draws-international-interest/>.
 - 71 Meghan E. Hall, “Innovation Draws International Interest,” *Army AL&T Magazine*, Winter 2022, 55-57, <https://asc.army.mil/armyalt/Winter2022/html/print/Winter-2022%20Download.pdf>.
 - 72 Department of the Army, Department of Defense Fiscal Year (FY) 2024 Budget Estimates: Army Justification Book Volume 2 of 3: Other Procurement, Army Communications and Electronics Equipment, Budget Activity 2 (Washington, DC: Department of the Army, March 2023), 472, <https://www.asafm.army.mil/Portals/72/Documents/BudgetMaterial/2024/Base%20Budget/Procurement/Other%20Procurement%20-%20BA%20%20-%20Communications%20and%20Electronics.pdf>.
 - 73 “How Russia is using Iranian killer drones to spread terror in Ukraine,” PBS, October 17, 2022, <https://www.pbs.org/newshour/world/how-russia-is-using-iranian-killer-drones-to-spread-terror-in-ukraine>
 - 74 “Germany to send seven additional Gepard tanks to Ukraine,” Reuters, December 2, 2022, <https://www.reuters.com/world/europe/germany-send-seven-additional-gepard-tanks-ukraine-spiegel-2022-12-02/>; and Usaid Siddiqui and Dalia Hatuqa, “Ukraine war updates: ‘Significant’ losses inflicted on Russia,” Al Jazeera, February 19, 2023, <https://www.aljazeera.com/news/liveblog/2023/2/19/russia-ukraine-live-news-west-unwilling-to-discuss-peace-efforts>.
 - 75 “Coyote,” Raytheon, n.d., <https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/coyote>. Reprinted with permission.
 - 76 “Leonidas,” Epirus, n.d., <https://company-91928.frontify.com/d/yDw2dYCKKTq1/media-assets/collection/7901>. Reprinted with permission.
 - 77 Ibid. Reprinted with permission.
 - 78 “Drone Buster,” U.S. Department of Defense, October 9, 2020, <https://www.defense.gov/Multimedia/Photos/igphoto/2002575160/>.
 - 79 “Drone Destroyer,” Marines, November 22, 2022, <https://www.marines.mil/Photos/igphoto/2003119632/>.
 - 80 “Raytheon’s High Energy Laser Weapon System (HELWS),” Edwards Air Force Base, n.d., <https://www>.

edwards.af.mil/News/Photos/igphoto/2002275360/.

- 81 Anvil, Anduril, October 5, 2023, reprinted with permission, <https://www.anduril.com/article/anvil-m-launch/>; LPWS, U.S. Army, n.d., https://asc.army.mil/web/portfolio-item/ms-c-ram_lpws/; Jordan Allen, M-SHORAD, U.S. Army photo by Cpt. Jordan Allen, April 23, 2021, https://www.army.mil/article/245530/m_shorad_system_bolsters_armys_air_defense_capabilities; THOR, U.S. Air Force photo by John Cochran, February 11, 2021, <https://www.afrl.af.mil/News/Article/2512426/army-partners-with-air-forces-thor-for-base-defense/>; and L-MADIS, U.S. Marine Corps photo by Lance Cpl. Dalton S. Swanbeck, November 13, 2018, <https://www.peols.marines.mil/Programs/Ground-Based-Air-Defense/Ground-Based-Air-Defense-Image-Gallery/igphoto/2002548481/>.
- 82 Colin Demarest, “Epirus wins \$66M Army contract for drone-frying Leonidas microwave kit,” C4ISRnet, January 23, 2023, <https://www.c4isrnet.com/unmanned/2023/01/23/epirus-wins-66m-army-contract-for-drone-frying-leonidas-microwave-kit/>.
- 83 Patrick Tucker, “Drones Shooting Microwave Rays Could Be the Drone Killers of Tomorrow,” Defense One, February 13, 2022, <https://www.defenseone.com/technology/2022/02/drones-shooting-microwave-rays-could-be-drone-killers-tomorrow/361933/>.
- 84 Jason Knight, “Countering Unmanned Aircraft Systems,” (master’s thesis, Naval Postgraduate School and Center for Homeland Defense and Security, December 2019), 81, <https://www.hsdl.org/c/abstract/?docid=834488>.
- 85 Ibid.
- 86 GNSS covers a variety of satellite positioning systems including GPS, GLONASS, Galileo, and Beidou.
- 87 Ibid.
- 88 “Army announces selection of interim C-sUAS systems,” U.S. Army.
- 89 “Dronebuster SNA,” FlexForce, updated 2022, <https://flexforce.us/wp-content/uploads/2021/08/2022-Dronebuster-SNA-Datasheet.pdf>; “Dronebuster Block 3,” FlexForce, updated 2022, <https://flexforce.us/wp-content/uploads/2021/08/2022-Dronebuster-Blk-3-Datasheet.pdf>.
- 90 Riad Kahwaji, “Autonomous systems integration, UAS threats dominate UMEX conference,” Breaking Defense, February 21, 2022, <https://breakingdefense.com/2022/02/autonomous-systems-integration-uas-threats-dominate-umex-conference/>.
- 91 Mobile platforms are defined by the ability to rapidly relocate and deploy. Maneuverable capabilities are even stricter, requiring sensing and fire control while on the move.

CHAPTER 3: THE CURRENT PATH

- 92 Adapted from a U.S. Army presentation at ADA Symposium, Director of Capabilities Development & Integration Directorate (CDID) & Army Capability Managers (ACM), September 28, 2022.
- 93 Andrew Feickert, *U.S. Army Short-Range Air Defense Force Structure and Selected Programs: Background and Issues for Congress*, CRS Report No. R46463 (Washington, DC: Congressional Research Service, July 2020), <https://sgp.fas.org/crs/weapons/R46463.pdf>.
- 94 Michael Shurkin, “How the Bundeswehr Should Spend Its Money,” War on the Rocks, March 21, 2022, <https://warontherocks.com/2022/03/how-the-bundeswehr-should-spend-its-money/>.
- 95 “Army Air & Missile Defense Hot Topic 2018 - Panel 1 - Developing Capabilities,” YouTube video, posted by Association of the U.S. Army, April 2, 2018, 15:00, https://www.youtube.com/watch?v=htN5pZVnrVA&ab_channel=AssociationoftheU.S.Army.

- 96 Nicole Thomas, JCO division chief for strategy and policy, has described the forthcoming institutionalization of C-sUAS across the 2023-2027 budget cycle. See Theresa Hitchens, “New Counter Drone Strategy Hits Esper’s Desk,” *Breaking Defense*, October 15, 2020, <https://breakingdefense.com/2020/10/new-counter-drone-strategy-targets-joint-force/>.
- 97 Paraphrased definitions of DOTMLPF from “DOTMLPF-P Analysis,” Defense Acquisition University, <https://www.dau.edu/acquipedia-article/dotmlpf-p-analysis>.
- 98 “Employ dedicated observers (conducting air guard techniques); Perform visual aircraft recognition training; Conduct air threat avoidance techniques; Establish a security force and quick reaction force; Establish an early warning organic sensor network; Conduct UAS reporting procedures; Perform cover and concealment; Select appropriate LSS UAS defeat mechanisms.” Department of the Army, *Counter Unmanned Aerial System (C-UAS)*, ATP 3-01.81 (Washington, DC: Department of Defense, August 2023), 1-3, <https://irp.fas.org/doddir/army/atp3-01-81.pdf>.
- 99 U.S. Army, *U.S. Army Air and Missile Defense Operations* (Washington, DC: Department of the Army, December 2020), https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN31339-FM_3-01-000-WEB-1.pdf.
- 100 Joint Chiefs of Staff, *Joint Publication 3-01*, V-5.
- 101 *Ibid.*, III-34.
- 102 Interviews with Army leaders.
- 103 Devon L. Suits, “Joint counter UAS office plans future demos after strong first evaluation,” U.S. Army, April 20, 2021, https://www.army.mil/article/245375/joint_counter_uas_office_plans_future_demos_after_strong_first_evaluation.
- 104 “AUSA 2022 | Warriors Corner - Department of Defense Counter Small UAS (C-sUAS) Initiatives,” YouTube video, posted by U.S. Army Professional Forum, October 13, 2022, 35:57, https://www.youtube.com/watch?v=eObma5y-G0o&ab_channel=U.S.ArmyProfessionalForum.
- 105 “Courseware and Capabilities Catalog,” Joint Knowledge Online, January 2023, https://www.jcs.mil/Portals/36/Documents/JKO/JKO_Course_Catalog.pdf?ver=jy-yABnnNzXvOIvC1bZbUg%3d%3d.
- 106 Mark Schauer, “U.S. Army Yuma Proving Ground hosts counter-UAS school,” U.S. Army, June 3, 2021, https://www.army.mil/article/247173/u_s_army_yuma_proving_ground_hosts_counter_uas_school.
- 107 “SUAS Master Trainer,” Fort Benning and The Maneuver Center of Excellence, U.S. Army, last updated June 30, 2021, <https://www.benning.army.mil/armor/316thcav/SUASMT/index.html>.
- 108 Major General Sean Gainey, “Joint C-sUAS Office (JCO) Overview,” Space and Missile Defense Symposium, Huntsville, Alabama, August 10, 2022, https://smdsymposium.org/wp-content/uploads/2017/08/Wed-0915-MG-Gainey-JCO_Overview_Briefing_August_2022_final.pdf.
- 109 Department of the Army, ATP 3-01.81, 2-5.
- 110 Justin Katz, “Marines mulling interceptor upgrade for MADIS to counter UAS,” *Breaking Defense*, January 3, 2022, <https://breakingdefense.com/2022/01/marines-mulling-interceptor-upgrade-for-madis-to-counter-uas/>.
- 111 Kelsey Reichmann, “C-UAS Training Academy Coming to Fort Sill,” *Defense Daily*, October 30, 2020, <https://www.defensedaily.com/c-uas-training-academy-coming-fort-sill/army/>.
- 112 Devon Suits, “Joint Counter-sUAS strategy to address need for improved technology,” U.S. Army, October 8, 2020, https://www.army.mil/article/239593/joint_counter_suas_strategy_to_address_need_for_improved_technology.

- 113 Reichmann, “C-UAS Training Academy Coming to Fort Sill.”
- 114 Rick Lewis, “Counter-Unmanned Aircraft System summit discusses drone implications,” U.S. Army, December 15, 2016, https://www.army.mil/article/179737/counter_unmanned_aircraft_system_summit_discusses_drone_implications.

COVER PHOTO SIMON WOHLFAHRT/AFP/GETTY IMAGES



1616 Rhode Island Avenue NW
Washington, DC 20036
202 887 0200 | [**www.csis.org**](http://www.csis.org)