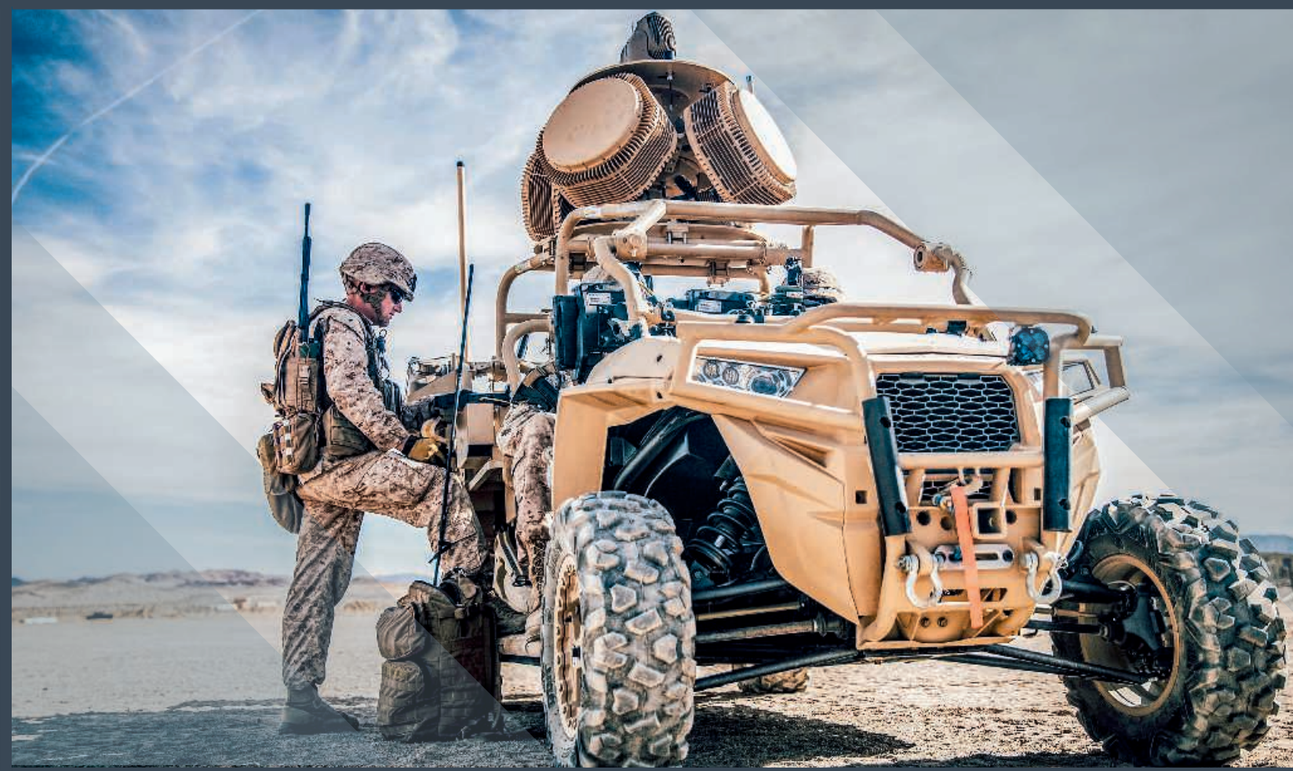

“The Department’s management structure and processes are not written in stone, they are a means to an end–empowering the warfighter with the knowledge, equipment and support systems to fight and win. Department leaders will adapt their organizational structures to best support the Joint Force.

U.S. Department of Defense

Counter-Small Unmanned Aircraft Systems Strategy

MESSAGE FROM THE ACTING SECRETARY

Challenges to the Joint Force are more complex and varied than at any other time. Rapid technological change has aided in disrupting the international rules-based order. Small unmanned aircraft systems (sUAS) were previously viewed as hobbyist toys, but today it is evident that the potential for hazards or threats has the ability to impact the Joint Force.

Our initial efforts were intended to meet the immediate needs of Services and combatant commanders. However, as technology and proliferation of sUAS continue to advance at a pace that challenges the Department's ability to respond effectively within current paradigms, it is evident that we cannot rely on materiel solutions alone. Instead, we must re-examine how to counter the growing challenges sUAS present to the Joint Force by considering and developing solutions that span the entirety of the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities—Policy (DOTMLPF-P) spectrum.

This strategy provides the framework for addressing sUAS across the spectrum from hazard to threat in the homeland, host nations, and contingency locations. As technology and systems evolve, this strategy will require ongoing assessments to ensure the Department keeps pace. Success will require unity of effort across all of DoD's stakeholders. The Military Departments, combatant commands, Joint Staff, and other DoD Components will maintain constant vigilance of sUAS and ensure the United States and its allies and partner nations maintain the most effective response.

Christopher C. Miller
Acting Secretary of Defense

This Page Intentionally Left Blank

U.S. Department of Defense
Counter-sUAS Strategy

Table of Contents

FRONT COVER
Marine Corps 1st Lt. Taylor Barefoot programs a counter-unmanned aircraft system on a Marine defense vehicle during a training exercise at Marine Corps Air Ground Combat Center Twentynine Palms, Calif., Nov. 13, 2018. (U.S. Marine Corps photo by Lance Cpl. Dalton Swanbeck)

BACK COVER
U.S. Army Soldier assigned to Headquarters and Headquarters Company, 3rd Battalion, 187th Infantry Regiment, 3rd Brigade Combat Team, 101st Airborne Division (Air Assault), launches the RQ-11 Raven during platoon live fire exercise at Fort Campbell, Ky., Jan. 25, 2018. (U.S. Army Photo by Capt. Justin Wright)

This Page Intentionally Left Blank

EXECUTIVE SUMMARY

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

In response to this challenge, the Department initially emphasized the deployment and employment of government and commercially-built materiel to address the immediate risks posed by sUAS; however, it resulted in many non-integrated, redundant solutions. Although the initial approach addressed near-term requirements, it also introduced challenges that complicated the Department's ability to keep pace with a constantly evolving problem. To address these challenges, the DoD requires a Department-wide holistic strategy for countering sUAS hazards and threats.

In November 2019, the Secretary of Defense designated the Secretary of the Army (SECARMY) as the DoD Executive Agent (EA) for Counter-Small Unmanned Aircraft Systems (C-sUAS, unmanned aircraft groups 1, 2, and 3). In his capacity as EA, the SECARMY established the Joint C-sUAS Office (JCO), which will lead, synchronize, and direct C-sUAS activities to facilitate unity of effort across the Department.

The DoD C-sUAS strategy provides the framework for addressing sUAS across the spectrum from hazard to threat in the homeland, host nations, and contingency locations. Department stakeholders will work collaboratively to achieve three strategic objectives: (1) enhance the Joint Force through innovation and collaboration to protect DoD personnel, assets, and facilities in the homeland, host nations, and contingency locations; (2) develop materiel and non-materiel solutions that facilitate the safe and secure execution of DoD missions and deny adversaries the ability to impede our objectives; and (3) build and broaden our relationships with allies and partners to protect our interests at home and abroad.

The Department will address these objectives by focusing on three lines of effort: Ready the Force; Defend the Force; and Build the Team. To Ready the Force, DoD will maximize current C-sUAS capabilities and use a risk-based approach to guide efficient and rapid development of a suite of materiel and non-materiel solutions to address emerging requirements. To Defend the Force, DoD will coordinate the delivery of joint capabilities underpinned by DOTMLPF-P consideration and synchronize the development of operational concepts and doctrine. Finally, as the global military partner of choice, DoD will Build the Team by leveraging its existing relationships, create new partnerships, and expand information sharing to meet emerging challenges.

Through the implementation of this strategy, the Department will successfully address the challenges posed by both hazard and threat sUAS operating within the U.S. homeland, in host nations, and in contingency locations. Commanders in each of these varied operating environments will have the solutions they need to protect DoD personnel, facilities, assets, and missions from both current and future sUAS threats.

INTRODUCTION

The United States faces threats from a variety of actors including strategic competitors, regional powers, weak or failed states, and non-state actors. Competitors are challenging U.S. interests across all domains and geographic regions by leveraging advances in technology such as sUAS to achieve their objectives. Although the most common use of sUAS in the homeland is for legitimate purposes such as entertainment, protection of commercial facilities, law enforcement, or firefighting, these systems may inadvertently place DoD personnel, facilities, and assets at risk through careless behavior within an already congested airspace. Even at the lower end of the conflict spectrum, malicious actors can adapt this technology to create more robust capability.

As the sUAS problem expanded across multiple areas of responsibility, the Department adopted an approach that pursued immediate C-sUAS materiel solutions to address the rapidly evolving challenge for U.S. forces at home and abroad. This approach emphasized the deployment and employment of government and commercially-built materiel to address the immediate risks posed by sUAS; however, it resulted in many non-integrated, redundant solutions. Although the initial approach addressed near-term requirements, it also introduced challenges that complicated the Department's ability to keep pace with a constantly evolving problem. To address these challenges, the DoD requires a holistic strategy for countering sUAS hazards and threats.

Central Challenge

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

Materiel solutions alone cannot counter threat sUAS or mitigate hazards. Protecting U.S. forces, allies, and partners requires that we examine our existing doctrine, training, equipment, and policy to identify any potential shortfalls to countering present and future sUAS threats. This means we must work horizontally across the Department to ensure that the perspectives and requirements of the many stakeholders (Joint Force,[1] allies, partners, etc.) are considered across the DOTMLPF-P spectrum while also working with other federal agencies and domestic entities to improve interoperability and integration of capabilities. The Department must provide commanders with the right equipment and with ready forces which are supported by appropriate training and doctrine in order to enable the Joint Force to collectively meet the sUAS challenge. Finally, we must integrate active defenses, passive defenses, or a combination along with materiel and non-materiel solutions using a risk-informed, tiered approach to ensure the protection and defense of our personnel, assets, and facilities.[2] When all of these elements are synchronized, our forces will be prepared to detect, identify, deter, and, if necessary, defeat threat sUAS.

[1] While the term "Joint Force" traditionally refers to the doctrinal definition from JP 3-0 (A force composed of elements, assigned or attached, of two or more Military Departments operating under a single joint force commander), its use in this strategy is intended to be inclusive of all DoD Components that have C-sUAS equities and/or conduct C-sUAS operations.

[2] Department of Defense, Deputy Secretary of Defense Memorandum, "Guidance for Use of Counter-UnmannedAircraft Technology Outside the United States to Protect DoD Personnel, Installations, Facilities, and Assets," 7 May 2020.

To successfully address the sUAS challenge, stakeholders across the Department will pursue three strategic objectives:

- Enhance the Joint Force through innovation and collaboration to protect DoD personnel, assets, and facilities in the homeland, host nations, and contingency locations;
- Develop materiel and non-materiel solutions that facilitate the safe execution of DoD missions and deny adversaries the ability to impede our objectives; and
- Build and broaden our relationships with allies and partners to protect our interests at home and abroad.

Meeting these objectives will require emphasis on rapid innovation, synchronization of materiel and non-materiel solutions across the Joint Force, and partnerships that are underpinned by interoperability, integration, and information sharing.

Jerome Ramirez and U.S. Air Force Staff Sgt. Michael Ingold brief Maj. Gen. Robert D. McMurry, AirForce Research Laboratory commander, on his teams' counter unmanned aerial system solution, Dec. 14, 2016, during the AFRL Commanders Challenge at the Nevada National Security Site, Las Vegas, NV., Dec. 13, 2016.
(U.S. Air Force photo by Wesley Farnsworth)

SECURITY ENVIRONMENT

Around the world, competitors are rapidly adopting sUAS into their military, civil, and commercial inventories. Both state and non-state actors are increasingly employing purpose-built military and consumer-grade sUAS to attack a range of targets including leadership, military facilities and forces, and critical infrastructure. As this pattern continues to evolve, the Joint Force will see these systems employed in more novel ways to contest U.S. military advantage. In addition to changes in the operating environment, three primary drivers have created the imperative for the Department to address sUAS: (1) the changing character of warfare; (2) emergent strategic competition; and (3) challenges to the U.S. military advantage.[3]

An unmanned aerial system (UAS), operated by U.S. Air Force Academy cadets and Johns Hopkins University engineers, flies near the guided-missile destroyer USS Jason Dunham (DDG 109) during exercise Black Dart, Sept. 20, 2016. (U.S. Navy photo by Mass Communication Specialist 1st Class Maddelin Angebrand)

Changing Character of Warfare

Commercial manufacturers and nation states are improving performance, reliability, and survivability of sUAS. Low cost systems are increasingly available around the world. These more capable systems have extended range, payload, and employment options. Some of these systems can fit in the palm of a hand, perform military missions, and conduct novel offensive or defensive operations not traditionally associated with the platform. Swarms of sUAS operating independently or augmented with manned systems, facial recognition algorithms, and high-speed digital communication networks, such as fifth generation cellular networks, will create new levels of complexity. The impending integration of artificial intelligence with autonomous sUAS will introduce yet another dramatic change to the character of warfare.

Emergent Strategic Competition

Hostile nation states have learned from the successes of non-state actors and the United States in the employment of sUAS. Some of these nations have become beneficiaries in this rapidly expanding market. Others are fielding purpose-built military and consumer-grade sUAS in large numbers, which provide scalable options for defensive and offensive operations. For China, the development of sUAS generates both an economic incentive and a military benefit. As a major producer of commercial and consumer sUAS, China is estimated to have 70 percent of the global market share.[4] Militarily, China's capabilities and reach will continue to grow as it invests heavily in developing and fielding advanced weapons. Russia is making sUAS platforms an integral part of its future warfare capabilities by improving its reconnaissance-fires complex and fielding reconnaissance and attack UAS.[5] Iranian proxies are actively conducting kinetic operations with sUAS. The 2019 attacks on key Saudi Arabian oil facilities demonstrated how sUAS can be used to attack and disrupt critical infrastructure.

[3] Department of Defense, National Defense Strategy 2018, p.3.

[4] Patrick McGee, "How the commercial drone market became big business," Financial Times, November 26, 2019.

[5] Senate Intelligence Committee, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats#, January 29, 2019.

Even if the U.S. military does not engage in direct conflict with Russia, China, or Iran, U.S. forces will likely encounter advanced sUAS equipment, concepts, doctrine, and tactics used by their surrogates in locations around the globe.

Challenges to the U.S. Military Advantage

Both at home and abroad, sUAS affect the operations of ground, naval, air, and space forces. With enhanced surveillance capability, malicious actors can collect critical intelligence on a unit's location, composition, and activity. This level of situational awareness can enable an adversary to degrade the Joint Force's freedom of maneuver. When these systems are weaponized, sUAS can present a precision strike capability; direct attacks using small munitions; provide laser designation for indirect fires or remote engagement by manned platforms; or deploy chemical, biological, and radiological agents.[6] Small UAS can provide the adversary flexibility by extending sensor coverage and communications over the horizon—increasing warning time and extending effective weapons range. They can also enable adversaries to conduct operations with greater presence while remaining at a distance. Small UAS not only create effects against U.S. forces within a single domain, but are able to operate across multiple domains—transitioning from the air to the land or sea and back again. Finally, sensitive data on unsecured systems are targets for a variety of sUAS cyberattacks, and adversaries can use sUAS to collect information, deliver malicious content, or enable kinetic attacks.

Domestically, the most likely use of adversarial sUAS will be the collection of intelligence against U.S. forces and facilities. The physical danger posed by sUAS strikes remains present as the result of malicious and intentional attacks or accidental damage caused by careless use. The 2015 incident with a commercial drone crashing on the White House lawn, unauthorized overflights of sensitive facilities, and the disruption of airport operations provide insight into potential attacks by a determined and capable adversary. A single successful strike on a high-value asset could affect Joint Force readiness by degrading the ability to project power and employ forces as needed. In locations where the Department does not control the airspace, the Joint Force is presented with additional challenges that require coordination with national airspace managers in a balanced approach to protect the safety and security of military operations.

The emergence of sUAS as both hazard and threat has complicated an already complex and challenging security environment. While fundamentally aircraft, sUAS exist in the gap between air defense, force protection, and airspace control across the operating environment continuum. The continued proliferation of these systems will challenge DoD's existing paradigm for how it addresses emergent technologies that may pose a threat to the force. The solution to countering sUAS in or around DoD facilities, missions, or personnel will vary based on where the incursion occurs along the spectrum of operations (see Figure 1).

The increased availability of inexpensive, capable sUAS is allowing government, industry, and the public to employ what was once available only to the military and a small number of dedicated hobbyists. These systems are the fastest growing segment of the aviation industry, and this growth has dramatically increased the risk of sUAS hazards for the military. Improvements in sensor miniaturization, battery technology, flight performance, and control mechanisms, along with reductions in price and regulations, have led to increased interest in

[6] Lt Col Jeffrey Lamport, COL (R) Anthony Scotto, "Countering the UAS Threat from a Joint Perspective," Joint Deployable Analysis Team, February 09, 2017.

their commercial utility. As new technology continues to improve capabilities, commercial applications will also expand. Large commercial entities are pursuing UAS operations, resulting in a dramatic proliferation of highly capable drones occupying U.S. airspace and overflying DoD installations in the United States and around the world. To adapt to these changes in the air domain, the DoD must adopt a posture of anomaly detection by seeking ways to highlight abnormal behavior and focus attention on those sUAS identified as potential threats and hazards. As the Department's policies and capabilities evolve in response to the technological changes, it must also address how these systems enable adversaries to project power in a variety of new ways. In the hands of non-state actors, sUAS can be adapted into a surveillance or weapons system that poses a security threat to the force. When flown by well-intentioned hobbyists and commercial operators, they can unintentionally pose a safety hazard to DoD installations and assets. Despite the fundamental differences between these two uses, both create risk for DoD.

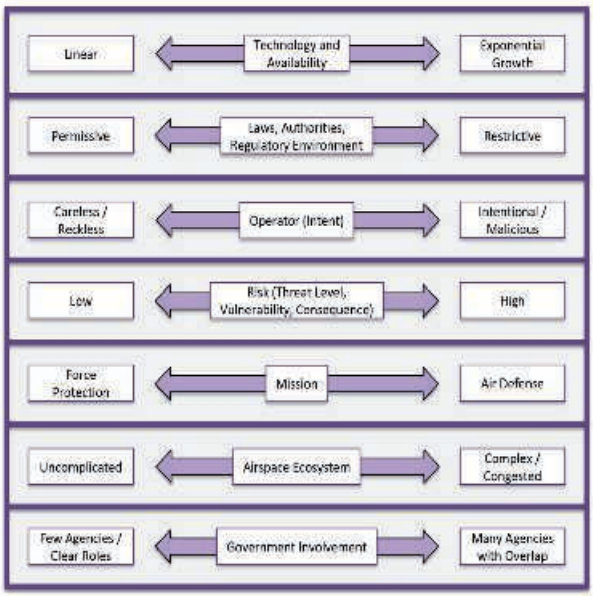

Figure 1: C-sUAS Spectrum of Operations

Three Operating Environments: Homeland, Host Nation, and Contingency Locations

Homeland. As the National Defense Strategy (NDS) recognized, the homeland is no longer a sanctuary. Though presence alone is not a threat, the ubiquity of sUAS operating within the United States presents a unique set of challenges. In the context of airspace management, commanders are challenged to determine the intent of sUAS operations through procedural and positive airspace control measures. The widespread use of sUAS as legitimate commercial platforms and hobbyist toys has resulted in efforts to integrate sUAS into the National Airspace System (NAS). However, the ability to effectively manage and track those platforms within the NAS has been slow to develop. These changes in both the security environment and the commercial sector have challenged our ability to adapt capabilities, authorities, and policies. Ongoing initiatives by the Federal Aviation Administration (FAA) to implement technologies like UAS Remote Identification as part of an effective Unmanned Aircraft System Traffic Management System are promising. However, until they are implemented, the burden of tactically detecting and identifying anomalous systems in the vicinity of U.S. forces and facilities remains the responsibility of installation commanders. The DoD conducts military operations, including C-sUAS activities, in the homeland amidst a complex environment. A framework of federal laws and regulations affects the C-sUAS actions DoD may take to protect domestic facilities and assets and requires coordination with other federal agencies. DoD installations are often surrounded by civilian populations and private property, and any harmful radio frequency, laser, microwave, or other energy directed outward from the installation has the potential to affect civilians or their property. Through its risk-based assessment, the Department must account for potential collateral effects of C-sUAS capabilities employed to protect its facilities. Furthermore, many existing laws and federal regulations were not designed to address sUAS as threats, and

the continued rate of technological change makes it difficult for the legal authorities to keep pace. This has inhibited our ability to employ effective defenses against these potential threats. The continued growth in commercial and hobbyist sUAS in the NAS will fundamentally alter the way airspace is managed, and the Department must work with relevant civil authorities to ensure the domestic use of C-sUAS systems adapts to this changing reality.

Host nations. Similar to the restrictions in the Homeland, host nation environments have a diverse array of statutes and regulations that could inhibit effective force protection efforts. Our bases and operations in host nations must work with local airspace control authorities while complying with local laws and obligations of treaties or other agreements.[7] As our allies and partners integrate sUAS into their national airspace systems, commanders abroad will need to adapt to the reality of increasing numbers of sUAS operating in the vicinity of U.S. forces. This creates a challenging operating environment where local commanders have varying authorities to take action to protect U.S. interests.

Contingency locations. Contingency locations are generally the least restrictive operating environment but potentially carry the highest risk. Even at the lower end of the spectrum of conflict, adversaries can adapt commercial sUAS for the accomplishment of military objectives such as intelligence, surveillance, and reconnaissance and kinetic strike. These adversaries may be able to adapt this technology to create more robust capability for cyber, electromagnetic warfare, or other effects. In this environment, the United States and its coalition partners will employ sUAS and manned aircraft to achieve military objectives, creating a highly congested but lesser controlled air domain.

U.S. Marine Corps Lance Cpl. Briar Purty, an infantryman with 3rd Battalion, 4th Marine Regiment, 1st Marine Division tests Drone Killer Counter-UAS Technology during Urban Advanced Naval Technology Exercise 2018 (ANTX-18) at Marine Corps Base Camp Pendleton, California, March 21, 2018. (U.S. Marine Corps photo by Lance Cpl. Rhita Daniel)

[7] Department of Defense, Deputy Secretary of Defense Memorandum, "Guidance for Use of Counter-Unmanned Aircraft Technology Outside the United States to Protect DoD Personnel, Installations, Facilities, and Assets," 7 May 2020.

A NEW STRATEGIC APPROACH

To address the central challenge, the Department must first evaluate the solutions in which we currently invest and the processes we leverage to field them. Part of that evaluation may require us to improve current capabilities and add layered defenses with new capabilities to address both sUAS adversarial threats and the hazards encountered from legitimate users. We must leverage the research, development, test and evaluation (RDT&E) centers of excellence to pursue the next generation of C-sUAS capabilities that will position the Joint Force for the future. We will rapidly develop innovative solutions while leveraging a risk-based assessment process.[8] This approach will enable us to make better-informed decisions that balance the effectiveness and efficiency of systems within budgetary realities. These actions will maximize our ability to provide the Joint Force with the most effective capabilities for use in the homeland, host nations, and contingency locations. We must also continuously evaluate the efficiency of our processes to provide effective materiel and non-materiel solutions to the Joint Force. Transformational processes, such as the Adaptive Acquisition Framework, can streamline efforts to meet the unique requirements of the C-sUAS problem set. However, some of our acquisition processes are optimized to support conventional operations with long-lead times for capability development. As the NDS states, "[t]he Department's management structure and processes are not written in stone, they are a means to an end–empowering the warfighter with the knowledge, equipment and support systems to fight and win."[9] If our processes do not adequately respond to the needs of a rapidly changing security environment, we must take a new approach.

Second, we must develop common materiel and non-materiel solutions. Those solutions must be supported by, and incorporated into, joint and Service doctrine and training standards that contribute to joint and combined arms operations.

Finally, we cannot rely on materiel and non-materiel solutions alone to protect our interests. We must leverage one of our biggest competitive advantages—being the partner of choice. With long-standing relationships across the globe, we can protect the United States and its interests and assist our allies and partner nations by prioritizing interoperability and information sharing.

This new approach will require all Department stakeholders to work collaboratively to achieve our strategic objectives: (1) enhance the Joint Force through innovation and collaboration to protect DoD personnel, assets, and facilities in the homeland, host nations, and contingency locations; (2) develop materiel and non-materiel solutions that facilitate the safe and secure execution of DoD missions and deny adversaries the ability to impede our objectives; and (3) build and broaden our relationships with allies and partners to protect our interests at home and abroad. As a Department we will address those objectives by focusing on three lines of effort (LOEs): Ready the Force; Defend the Force; and Build the Team.

[8] Department of Defense, Deputy Secretary of Defense Memorandum, "Risk-Based Assessment in Support of Counter-Unmanned Aircraft Activities to Protect DOD Facilities and Assets," 7 May 2020.

[9] Department of Defense, National Defense Strategy 2018, p. 10.

Joint Counter-sUAS Office

In 2019, the Joint C-sUAS Office (JCO) was established to lead, synchronize, and direct C-sUAS activities. In this role, the JCO will support the development and oversight of joint C-sUAS doctrine, requirements, materiel, training standards, and capabilities to establish joint solutions with a common architecture to address current and future emerging sUAS threats. Through the JCO, the Department will ensure there is consistency of approach, technology, operational constructs, and developmental intent for joint C-sUAS solutions. In the Department's ongoing effort to reduce unnecessary redundancy, this office will coordinate across many organizations to ensure we avoid duplication of effort and maximize efficiencies and effectiveness of program activities and developmental efforts.[10]

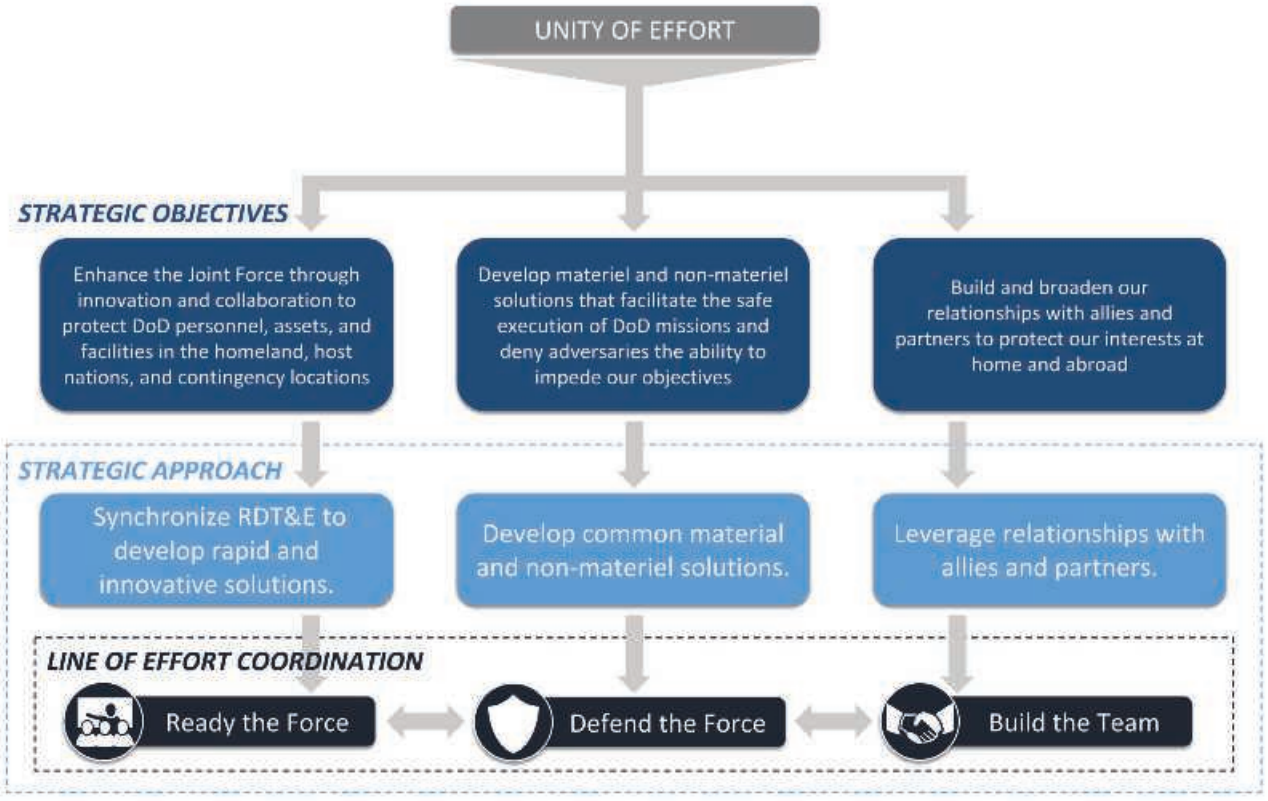

Figure 2: C-sUAS Unity of Effort

[10] Ibid., p. 9-10. Services will develop and provide Service-unique requirements to the DOD EA for C-sUAS to support materiel, doctrine, and training. The Secretary of the Army, as the EA, will provide oversight of unique C-sUAS requirements developed by the Military Departments/Services, Defense Agencies, and DoD Field Activities.

READY THE FORCE

Line of Effort 1: READY THE FORCE

We will maximize our current C-sUAS capabilities and use a risk-based approach to guide the efficient and rapid development of a suite of solutions to address emerging requirements.[11] Across the Department, we will remain responsive to the needs of combatant commands by benchmarking and improving existing joint capabilities against the current worldwide sUAS threat. To protect our forces, facilities, and assets, our C-sUAS systems will enable actionable UAS reporting, identification, and dissemination to the appropriate authorities to support attribution and law enforcement efforts.[12] As technological advancements and emergent threats continue to evolve, we will position ourselves for the future by focusing on systems with a common architecture. Informed by acquisition and operationally-relevant threat assessments, we will synchronize Science & Technology (S&T) strategies and investments across the Department. Our developmental efforts will consider current and projected needs, have application across the operating environments, and deploy upgrades or new systems to the Joint Force at the speed of relevance.

Figure 3: Line of Effort 1

1.1 Coordinate development of threat assessments that can inform current and future joint capability requirements. We will establish enduring intelligence requirements and priorities that will support the development of threat analysis-informed capabilities. The Defense Intelligence Enterprise (DIE) will cooperate with the larger intelligence community to provide timely and informative threat assessments for a range of stakeholders across the Department. Specifically, the DIE will make the unique C-sUAS requirements of combatant commanders and Services a priority. These assessments will be both descriptive and predictive and cover the range of threats from violent extremist organizations and criminal elements to near-peer adversaries targeting U.S. personnel, assets, and facilities at home and abroad. Finally, intelligence subject matter experts will provide proactive and reactive support to combatant commanders and Services to identify and address adversarial threat sUAS capabilities.

[11] Department of Defense, Deputy Secretary of Defense Memorandum, "Guidance for Employing Non-technical solutions for prevention and reducing the risk of unmanned aircraft incidents," May 7, 2020.

[12] Sharing intercepted or acquired UAS communication with law enforcement agencies (and with Federal regulatory agencies undertaking enforcement activities) is permitted under 10 U.S.C. 130i if it would fulfill a function of the Department of Defense, if it is required by law or regulation, or if it would support a criminal or civil investigation of illicit UAS actors, including identifying illicit UAS actors as part of such an investigation. Information acquired outside the United States may be shared with host country authorities in accordance with applicable U.S. and international law, including treaties and agreements.

1.2 Synchronize DoD S&T investments and accelerate development of key joint C-sUAS technologies. Guided by sUAS threat assessments, the Department will identify acceptable levels of risk based on threat level, vulnerability, and consequence across the three distinct operating environments.[13] We must improve our ability to respond to emergent threat sUAS and reduce tactical and operational surprise in contingency locations. Further, we must prioritize the development of technology that provides reliable detection, tracking, and identification capability in the homeland and host nations where the vast majority of our forces operate. The expertise, guidance, and recommendations from Defense Agencies, DoD Field Activities, and Military Departments will inform investment to promising joint C-sUAS technologies and innovative commercial solutions.

Amphibious transport dock ship USS Portland (LPD 27) successfully disabled an unmanned aerial vehicle (UAV) with a Solid State Laser - Technology Maturation Laser Weapon System Demonstrator (LWSD) MK 2 MOD 0.
(U.S. Navy video from U.S. Pacific Fleet Public Affairs)

1.3 Develop common information sharing architecture solutions to address current and future threat sUAS. The materiel component of our layered defense must be adaptable, integrated, and interoperable. The need to develop standalone C-sUAS systems to counter immediate, narrow, singular sUAS threats evolved into a requirement for more flexible, multi-threat C-sUAS solutions. As we upgrade current C-sUAS capabilities and develop future solutions that will be employed across all operating environments, our systems must share a common architecture and be both complementary and interoperable. Our materiel solutions must draw from standardized interfaces that enable joint and multilateral information sharing that is interoperable and capable of plug-and-play. Additionally, we will develop a centralized sUAS threat data architecture to inform the Department's work in developing and validating C-sUAS requirements. With a common architecture and a common threat picture, we will increase agility and responsiveness in addressing emergent threat sUAS.

1.4 Establish joint C-sUAS Test and Evaluation (T&E) protocols, standards, and methodologies. The Department will leverage its threat assessments and centralized data repositories to enable joint solutions capable of countering current and future sUAS threats. The DoD will ensure these systems are capable of integrating into a layered defense by establishing appropriate testing standards that evaluate capabilities in operationally relevant conditions and environments, against operationally relevant threats. Through T&E, experiments, assessments, and testing protocols, these solutions will be validated and integrated as part of the layered defense.

[13] Department of Defense, Deputy Secretary of Defense Memorandum, "Risk-Based Assessment in Support of Counter-Unmanned Aircraft Activities to Protect DOD Facilities and Assets," May 7, 2020.

DEFEND THE FORCE

Line of Effort 2: DEFEND THE FORCE

Figure 4: Line of Effort 2

Our commanders must have mission-ready forces that are able to deter and defeat sUAS threats. Combatant commanders must be prepared to win in future conflicts against the full range of threats, from non-state actors to near-peer adversaries. Commanders of DoD installations and missions must be prepared to protect their critical assets on a daily basis, whether from the hazards posed by negligent operators or actual threats from malicious actors. We will develop common, integrated C-sUAS materiel and non-materiel solutions that will strengthen active and passive defenses across all three operating environments. Non-materiel solutions will span across the DOT_LPF-P spectrum, with priority given to non-technical solutions such as concepts, doctrine, and training that are effective in preventing and reducing risks from sUAS. Combatant commanders will develop regional concepts of operations, providing specific guidance on the integration of C-sUAS across air defense, force protection, and airspace control functions that are appropriate for each of the three operating environments. Through Service coordination and in conjunction with the Military Training Capabilities Group (MTCG), we will create common training guidelines and qualification standards that are responsive to emerging threat sUAS and evolving C-sUAS capabilities. However, the scope and scale of sUAS proliferation cannot be addressed through these solutions alone. Countering threat sUAS demands greater interoperability with existing organic capabilities of the Joint Force. Through combined arms operations, the Joint Force will employ effects from all domains to degrade, disrupt, or destroy adversary's capabilities.

2.1 Deliver joint capabilities that are synchronized across DOTMLPF-P. Strengthening our defenses against sUAS will require additional risk-based investment across the Services.[14] To achieve the greatest possible buying power, we will develop and deliver a family of capabilities based on approved joint requirements documents. To maximize our investments, the new suite of capabilities will be underpinned by synchronized DOTMLPF-P efforts. To do otherwise creates the unacceptable risk of exacerbating shortfalls that already exist. DOTMLPF-P synchronization must also be applied to the integration of defensive and offensive capabilities. Non-materiel solutions such as common tactics, techniques, and procedures; training; and education will enable better integration of existing capabilities of the Joint Force. A synchronized C-sUAS multi-domain approach must leverage space, air, maritime, land, cyber, and electromagnetic capabilities simultaneously to yield operational advantages. This will enable us to leverage prior investments in offensive capabilities that can be employed to degrade, disrupt, or destroy sUAS. As a result, Joint Force commanders will have expanded options to deter, deny, and defeat through the use of layered active and passive defense in concert with offensive operations.

2.2 Develop operational concepts and doctrine to improve the Joint Force's competitive edge. New joint operational concepts will identify required non-materiel capabilities for the Joint Force. These concepts will

[14] Ibid.

cover the spectrum of operations, from peacetime to large scale combat operations, and address each of the three operating environments. Joint operational concepts for C-sUAS will emphasize the value of employing a combined arms team approach in appropriate circumstances and the value of utilizing cross-domain effects. Additionally, the concepts will identify ways to mitigate hazards during peacetime and counter the challenges that adversaries will create with sUAS. Joint concepts will also identify required capabilities for the Joint Force that will improve freedom of action and control of the air domain in contingency locations through synchronization of air defense, force protection, and airspace control. Once developed and approved, they will be incorporated into Service and joint doctrine.

2.3 Establish joint training standards, refine existing training content, and transition to Service training systems. Training is the cornerstone of readiness, whether for combat or for daily protection of critical DoD missions. To ensure training is responsive to emerging threat sUAS and evolving C-sUAS capabilities, we will create common training guidelines and qualification standards in conjunction with the MTCG and the Secretary of Defense's directed Joint Operational Training Infrastructure strategy. Simultaneous with the development of standards, we will improve the quality of training, develop sUAS awareness training for all members of the Department, and develop content applicable across the Joint Force. Services will use their expertise in training development to increase the quality and rigor of individual and unit training. This effort will build upon existing investments in training that were developed to support rapid materiel fielding. As common C-sUAS training functions transition to joint management, all Department agencies and Services will ensure training activities continue to meet combatant commander needs. The Services will also ensure they continue to meet their Service-specific training responsibilities and common training needs.

Troopers assigned to 1st Squadron, 3rd Cavalry Regiment, operate the Drone Defender during a counter-unmanned aerial system drill while deployed to Iraq, Oct. 30, 2018. (U.S. Army photo by MAJ Jason Welch)

BUILD THE TEAM

Line of Effort 3: BUILD THE TEAM

Figure 5: Line of Effort 3

One of our biggest competitive advantages militarily is being the partner of choice and a global leader. We will leverage existing relationships, create new partnerships, and expand information and data sharing. The Department will partner closely with the FAA in the homeland and with national airspace managers abroad to support the integration of sUAS into the future aviation ecosystem. We will advocate the development of sUAS identification technologies that will facilitate anomaly detection and improve air safety. When necessary, the Joint Force must have the capability to conduct C-sUAS joint and combined arms operations where appropriate in multi-national operations to identify, facilitate attribution, deter threats, and in all instances protect identified DoD facilities and assets in the homeland, in host nations, and in contingency locations.[15] The Joint Force will advocate for mutually beneficial policies, authorities, and agreements that enable international cooperation and partnering. To do so, we will improve partnerships at home and abroad; sustain and strengthen allies and partner nations; and rapidly develop and deploy C-sUAS innovative and interoperable solutions faster than our adversaries through advocacy and collaboration with allies, partner nations, national security innovation base (NSIB), domestic entities, federal agencies, and other non-federal entities (NFE). By developing adaptive agreements with our allies and partner nations as well as federal and domestic law enforcement agencies to streamline the approval processes, the Department can enable collaborative technology development that keeps pace with the rapidly changing nature of the threat. We will clarify roles and missions in support of C-sUAS activities and where feasible, invest in systems that enable interoperability with domestic entities and integration with other federal agencies.

3.1 Partner with the national security innovation base (NSIB) and other non-federal entities (NFE) to facilitate rapid development of joint capabilities to mitigate hazardous sUAS and deter and defeat threat sUAS. The Joint Force must attract new partners and engage with rising technology leaders to defend against evolving threats from non-state actors to near-peer competitors. We will collaborate and harness the NSIB and NFE partnerships to rapidly develop C-sUAS capabilities to reduce gaps and rapidly expand manufacturing throughput to exploit new technological advancements. Establishing a strong partnership between the DoD and the NSIB will ensure a healthy U.S. commercial innovation base for the future. These partnerships will enable us to accelerate the development of solutions and provide the Joint Force and DoD Components with effective countermeasures for sUAS hazards and threats. We will also seek to establish new agreements with civilian organizations and expand multilateral collaboration.

[15] Sharing with law enforcement agencies is permitted under 10 U.S.C. 130i if it would fulfill a function of the Department of Defense, if it is required by law or regulation, or if it would support a criminal or civil investigation of illicit UAS actors, including identifying illicit UAS actors as part of such an investigation. Information acquired outside the United States may be shared with host country authorities in accordance with applicable U.S. and international law, including treaties and agreements.

3.2 Sustain, strengthen, and maximize interoperability with allies and partner nations. To protect our shared interests, the Joint Force must be interoperable with its allies and partner nations. We will continue to build partner C-sUAS capacity and capability. Through the development of mutually beneficial local policies and by leveraging programs with key partner nations, the Department will improve its ability to protect U.S. personnel, assets, and facilities in host nations. Cooperative efforts with allies and partners will include opportunities for technology exchanges, shared investments, and common system standards. We will proactively support the Joint Force to enhance C-sUAS information sharing and synchronization efforts with host nations to influence unimpeded approval and authorities for access to the electromagnetic spectrum. We will expedite the fielding of C-sUAS solutions through early acquisition planning with appropriate safeguards to prevent the loss of technological advantages to our adversaries. Additionally, the Department will establish adaptive agreements, refine the approval process and the procurement mechanisms to expedite the standard channels, and abbreviate the processes to facilitate rapid acquisition and distribution by leveraging existing tools.

We will proactively engage partner nations and allies to conduct combined C-sUAS RDT&E efforts and expand experimentation opportunities to conduct demonstrations and testing of new technology advancements. We will integrate export requirements early into the development of C-sUAS systems in order to compress the timeline to share technology. Finally, we will advance foreign military sales and direct commercial sales of C-sUAS equipment to bolster a competitive U.S. commercial market and strengthen our collective defense.

3.3 Coordinate with domestic entities to enable interoperability and maximize integration with our federal agencies to protect DoD facilities and assets in the homeland. The Joint Force must enhance C-sUAS information sharing and synchronize actions with our federal and domestic law enforcement agencies and other partners, as required by law, to improve predictive analytics, actionable sUAS reporting, identification, and dissemination to the appropriate authorities to support attribution and prosecution of illicit and reckless sUAS actors. We will work with our federal partners to establish adaptive agreements that improve airspace management and enhance their ability to execute C-sUAS authorities and missions independently and jointly. We will coordinate our C-sUAS investments leveraging rapid manufacturing and prototyping authorities and adapt existing federal agency acquisition authorities as necessary to leverage the combined buying power of the U.S. Government. We will also improve coordination and shared strategic awareness by enhancing information and data sharing to increase our airspace control, air defense, and overall force protection.

U.S. Marine Corps Sgt. Joseph Howell conducts operation checks on a C-UAS system in Southwest Asia, April 22, 2019. (U.S. Marine Corps photo by Cpl. Alina Thackray)

CONCLUSION

At home and abroad, U.S. forces will increasingly encounter sUAS and must be able to detect, track, identify, and, if necessary, deter, deny, or defeat them. Even legitimate but reckless use of these systems in the vicinity of DoD forces and facilities can impede our operations. Addressing the range of actors and operating environments will require us to align training, doctrine, materiel, policies, and authorities.

To keep pace with rapidly evolving technology, the Department will evaluate its current processes and make deliberate risk-based investment choices while providing the Joint Force with the range of support required across the DOTMLPF-P spectrum. This evaluation will drive investments in systems that are interoperable, share a common and secure architecture, and are able to counter multiple threats. If our processes do not enable us to effectively provide the Joint Force with "the knowledge, equipment and support systems to fight and win," then we must reimagine how to better support them in a rapidly changing technology and security environment.[16]

Guided by our Strategic Objectives, we will develop and deploy effective systems, complemented with doctrine and training products, that provide the Joint Force with capabilities to successfully counter current and future sUAS threats and hazards as part of a layered defense. As we leverage our RDT&E and intelligence assets, we will expand the competitive space to protect our interests across the globe. Finally, we will work with our allies and partners to develop a shared understanding of threats, vulnerabilities, and interoperability needs. Through this holistic approach, the Department will ensure the Joint Force is both ready to meet today's challenges and prepared for the future.

A view of Travis Air Force Base, Calif.'s Intel Shooting Star Drone light show where Travis families were shown the choreographed capabilities of over 500 drones during an Independence Day celebration, July 5, 2018.
(U.S. Air Force photo by Airman 1st Class Christian Conrad)

[16] Department of Defense, National Defense Strategy 2018, p. 10.

This Page Intentionally Left Blank

This Page Intentionally Left Blank

ANNEX A. GLOSSARY

C-sUAS	counter-small unmanned aircraft systems
DIE	Defense Intelligence Enterprise
DoD	Department of Defense
DOTMLPF-P	doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy
EA	Executive Agent
FAA	Federal Aviation Administration
JCO	Joint Counter-Small Unmanned Aircraft Systems Office
LOE	Line of Effort
MTCG	Military Training Capabilities Group
NAS	National Airspace System
NDS	National Defense Strategy
NFE	non-federal entity
NSIB	National Security Innovation Base
OSD	Office of the Secretary of Defense
RDT&E	research, development, test, and evaluation
S&T	science and technology
SECARMY	Secretary of the Army
sUAS	small unmanned aircraft systems
T&E	test and evaluation
UAS	unmanned aircraft systems
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment

Terms and Definitions

adversary. A party acknowledged as potentially hostile to a friendly party and against which the use of force may be envisaged. (JP 3-0)

air defense. Defensive measures designed to destroy attacking enemy aircraft or aerodynamic missiles, or to nullify or reduce the effectiveness of such attack. Also called **AD**. (JP 3-01)

air domain. The atmosphere, beginning at the Earth's surface, extending to the altitude where its effects upon operations become negligible. (JP 3-30)

ANNEX A. GLOSSARY

airspace control. Capabilities and procedures used to increase operational effectiveness by promoting the safe, efficient, and flexible use of airspace. (JP 3-52)

artificial intelligence. the ability of machines to perform tasks that normally require human intelligence – for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action – whether digitally or as the smart software behind autonomous physical systems. (2018 DoD Artificial Intelligence Strategy)

assessment. 1. A continuous process that measures the overall effectiveness of employing capabilities during military operations. 2. Determination of the progress toward accomplishing a task, creating a condition, or achieving an objective. 3. Analysis of the security, effectiveness, and potential of an existing or planned intelligence activity. 4. Judgment of the motives, qualifications, and characteristics of present or prospective employees or "agents." (JP 3-0)

attribution. 1. Labeling some entity as either the cause or effect of another item. (Black's Law Dictionary) 2. The linkage of events, locations, items, signatures, nefarious intent, and persons of interest. (derived from forensic-enabled intelligence definition in JP 2-0

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. (JP 1)

combatant commander. A commander of one of the unified or specified combatant commands established by the President. (JP 3-0)

combined. A term identifying two or more forces or agencies of two or more allies operating together. (JP 3-16)

contingency location. A non-enduring location outside of the United States that supports and sustains operations during contingencies or other operations and is categorized by mission life-cycle requirements as initial, temporary, or semi-permanent. (JP 4-04)

countermeasures. That form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. (JP 3-13.1)

critical infrastructure. The infrastructure and assets vital to a nation's security, governance, public health and safety, economy, and public confidence. (JP 3-27)

critical intelligence. Intelligence that is crucial and requires the immediate attention of the commander. (JP 2-0)

defense intelligence enterprise. The collection of (the) Department of Defense intelligence, counterintelligence and security communities.

ANNEX A. GLOSSARY

Department of the Army. The executive part of the Department of the Army at the seat of government and all field headquarters, forces, Reserve Component, installations, activities, and functions under the control or supervision of the Secretary of the Army. (JP 1)

Department of Defense Components. The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff and the Joint Staff, the combatant commands, the Office of the Inspector General of the Department of Defense, the Department of Defense agencies, Department of Defense field activities, and all other organizational entities in the Department of Defense. Also called **DoD Components.** (JP 1)

deter. To prevent action by the existence of a credible threat of unacceptable counteraction and/or belief that the cost of action outweighs the perceived benefits. (Derived from JP 3-0)

DoD Executive Agent. The Head of a DoD Component to whom the Secretary of Defense or the Deputy Secretary of Defense has assigned specific responsibilities, functions, and authorities to provide defined levels of support for operational missions, or administrative or other designated activities that involve two or more of the DoD Components. (DoDD 5101.1)

effect. 1. The physical or behavioral state of a system that results from an action, a set of actions, or another effect. 2. The result, outcome, or consequence of an action. 3. A change to a condition, behavior, or degree of freedom. (JP 3-0)

exploitation. 1. Taking full advantage of success in military operations, following up initial gains, and making permanent the temporary effects already created. 2. Taking full advantage of any information that has come to hand for tactical, operational, or strategic purposes. 3. An offensive operation that usually follows a successful attack and is designed to disorganize the enemy in depth. (JP 2-01.3)

force. 1. An aggregation of military personnel, weapon systems, equipment, and necessary support, or combination thereof. 2. A major subdivision of a fleet. (JP 1)

force protection. Preventive measures taken to mitigate hostile actions against Department of Defense personnel (to include family members), resources, facilities, and critical information. (JP 3-0)

hazards. 1. A danger or risk. 2. A condition that could foreseeably cause or contribute to an accident, unintentionally or by otherwise careless manner creates a danger. (derived from OSD Policy)

homeland. The physical region that includes the continental United States, Alaska, Hawaii, United States territories, and surrounding territorial waters and airspace. (JP 3-28)

host nation. A nation which receives forces and/or supplies from allied nations and/or North Atlantic Treaty Organization to be located on, to operate in, or to transit through its territory. (JP 3-57)

ANNEX A. GLOSSARY

identification. 1. The process of determining the friendly or hostile character of an unknown detected contact. 2. In arms control, the process of determining which nation is responsible for the detected violations of any arms control measure. 3. In ground combat operations, discrimination between recognizable objects as being friendly or enemy, or the name that belongs to the object as a member of a class. Also called ID. (JP 3-01)

intelligence. 1. The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. 2. The activities that result in the product. 3. The organizations engaged in such activities. (JP 2-0)

intelligence requirement. 1. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. 2. A requirement for intelligence to fill a gap in the command's knowledge or understanding of the operational environment or threat forces. (JP 2-0)

integration. 1. In force protection, the synchronized transfer of units into an operational commander's force prior to mission execution. (JP 1) 2. The arrangement of military forces and their actions to create a force that operates by engaging as a whole. (JP 1) 3. In photography, a process by which the average radar picture seen on several scans of the time base may be obtained on a print, or the process by which several photographic images are combined into a single image. (JP 1) 4. In intelligence usage, the application of the intelligence to appropriate missions, tasks, and functions. See also force protection. (JP 2-01)

interoperability. 1. The ability to act together coherently, effectively, and efficiently to achieve tactical, operational, and strategic objectives. (JP 3-0) 2. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and/or their users. (JP 6-0)

joint. Connotes activities, operations, organizations, etc., in which elements of two or more Military Departments participate. (JP 1)

joint force. A force composed of elements, assigned or attached, of two or more Military Departments operating under a single joint force commander. (JP 3-0)

joint staff. 1. The staff of a commander of a unified or specified command, subordinate unified command, joint task force, or subordinate functional component (when a functional component command will employ forces from more than one Military Department), that includes members from the several Services comprising the force. 2. (capitalized as Joint Staff) The staff under the Chairman of the Joint Chiefs of Staff that assists the Chairman and the other members of the Joint Chiefs of Staff in carrying out their responsibilities. (JP 1)

leverage. In the context of planning, a relative advantage in combat power and/or other circumstances against the enemy or adversary across any variable within or impacting the operational environment sufficient to exploit that advantage. (JP 5-0)

ANNEX A. GLOSSARY

line of effort. In the context of planning, using the purpose (cause and effect) to focus efforts toward establishing operational and strategic conditions by linking multiple tasks and missions. Also called **LOE** (JP 5-0)

maritime domain. The oceans, seas, bays, estuaries, islands, coastal areas, and the airspace above these, including the littorals. (JP 3-32)

materiel. All items necessary to equip, operate, maintain, and support military activities without distinction as to its application for administrative or combat purposes. (JP 4-0)

Military Department. One of the departments within the Department of Defense created by the National Security Act of 1947, which are the Department of the Army, the Department of the Navy, and the Department of the Air Force. (JP1)

mission. 1. The task, together with the purpose, that clearly indicates the action to be taken and the reason, therefore. (JP 3-0) 2. In common usage, especially when applied to lower military units, a duty assigned to an individual or unit; a task. (JP 3-0) 3. The dispatching of one or more aircraft to accomplish one particular task. (JP 3-30)

national security innovation base. The American network of knowledge, capabilities, and people-including academia, National Laboratories, and the private sector that turns ideas into innovations, transforms discoveries into successful commercial products and companies, and protects and enhances the American way of life. (2017 NSS, page 21)

non-federal entity. Any private entity, commercial industry, non-federal government and domestic entity, Non-Governmental Organizations (NGOs), or International Organizations (IOs). (Derived from 6 USC 1501 and 25APR2013 OSD/VCJCS "Public Private Partnerships Supporting the DoD Mission Memo")

-private entities includes any corporate social foundations, academia, think-tanks, professional associations.

-non-federal government and domestic entities includes any state, tribal, or local government and any political subdivision, agency, department, or component thereof of the District of Columbia, the Commonwealth of Puerto Rico, the United States Virgin Islands, Guam, American Samoa, the Northern Mariana Islands, and any other territory or possession of the United States.

-excludes any entities affiliated with or sponsored by any component of a foreign power as defined in section 1801 of title 50.

objective. 1. The clearly defined, decisive, and attainable goal toward which an operation is directed. 2. The specific goal of the action taken which is essential to the commander's plan. (JP 5-0)

ANNEX A. GLOSSARY

operation. 1. A sequence of tactical actions with a common purpose or unifying theme. (JP 1) 2. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission. (JP 3-0)

partner nation. 1. A nation that the United States works with in a specific situation or operation. (JP 1) 2. In security cooperation, a nation with which the Department of Defense conducts security cooperation activities. (JP 3-20)

personnel. Individuals required in either a military or civilian capacity to accomplish the assigned mission. (JP 1-0)

procedures. Standard, detailed steps that prescribe how to perform specific tasks. (CJCSM 5120.01)

protection. Preservation of the effectiveness and survivability of mission-related military and nonmilitary personnel, equipment, facilities, information, and infrastructure deployed or located within or outside the boundaries of a given operational area. (JP 3-0)

reconnaissance. A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area. (JP 2-0)

Service. A branch of the Armed Forces of the United States, established by act of Congress, which are: the Army, Marine Corps, Navy, Air Force, Space Force, and Coast Guard. (JP 1)

small unmanned aircraft system. The system, within UA Groups 1-3, whose components include the necessary equipment, network, and personnel to control an unmanned aircraft. Also called sUAS. (Derived from JP 3-30 and DoDD 3800.01)

strategy. A prudent idea or set of ideas for employing the instruments of national power in a synchronized and integrated fashion to achieve theater, national, and/or multinational objectives. (JP 3-0)

strike. An attack to damage or destroy an objective or a capability. (JP 3-0)

support. 1. The action of a force that aids, protects, complements, or sustains another force in accordance with a directive requiring such action. 2. A unit that helps another unit in battle. 3. An element of a command that assists, protects, or supplies other forces in combat. (JP 1)

surveillance. The systematic observation of aerospace, cyberspace, surface, or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means. (JP 3-0)

ANNEX A. GLOSSARY

synchronization. 1. The arrangement of military actions in time, space, and purpose to produce maximum relative combat power at a decisive place and time. 2. In the intelligence context, application of intelligence sources and methods in concert with the operation plan to answer intelligence requirements in time to influence the decisions they support. (JP 2-0)

tactics. The employment and ordered arrangement of forces in relation to each other. (CJCSM 5120.01)

techniques. Non-prescriptive ways or methods used to perform missions, functions, or tasks. (CJCSM 5120.01)

threat analysis. In antiterrorism, a continual process of compiling and examining all available information concerning potential terrorist activities by terrorist groups which could target a facility. (JP 3-07.2)

threat assessment. An intelligence assessment that details the threat, capabilities, and intentions of adversaries' UAS capabilities (current and future). (Derived from JP 2-0)

unity of effort. Coordination and cooperation toward common objectives, even if the participants are not necessarily part of the same command or organization, which is the product of successful unified action. (JP 1)

unmanned aircraft. An aircraft that does not carry a human operator and is capable of flight with or without human remote control. Also called **UA**. (JP 3-30)

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

U.S. forces. All Armed Forces (including the Coast Guard) of the United States, any person in the Armed Forces of the United States, and all equipment of any description that either belongs to the US Armed Forces or is being used (including Type I and II Military Sealift Command vessels), escorted, or conveyed by the US Armed Forces. (JP 1)

vulnerability. 1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. (JP 3-01) 2. The characteristics of a system that can cause it to be degraded (incapability to perform the designated function or mission) as a result of being subjected to a certain level of effects in an unnatural (man-made) hostile environment. (JP 3-60) 3. In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 3-13)

working group. An enduring or ad hoc organization within a headquarters consisting of a core functional group and other staff and component representatives whose purpose is to provide analysis on the specific function to users. Also called **WG**. (JP 3-33)

ANNEX B. GOVERNANCE

The Secretary of Defense designated the SECARMY as the DoD EA for C-sUAS. The Under Secretary of Defense for Acquisition and Sustainment (USD [A&S]) is the cognizant Office of the Secretary of Defense (OSD) Principal Staff Assistant to oversee the designation. DoD Directive 3800.01E, "DoD Executive Agent for Counter Small Unmanned Aircraft Systems for Unmanned Aircraft Groups 1, 2, and 3" prescribes the governance structure for the C-sUAS effort. This annex provides an overview of the governance. The stakeholders include: OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD. Coordination with other federal partners and non-federal security, particularly in the Homeland, will be necessary. An Executive Steering Committee, chaired by the Vice Chief of Staff of the Army and co-chaired by the USD(A&S), will assist the Secretary of Defense in assessing joint military C-sUAS military capabilities; identifying, approving, and prioritizing gaps in such capabilities; reviewing and validating proposed C-sUAS capabilities; and endorsing joint performance requirements.

The Joint C-sUAS Office has been established to lead, synchronize, and direct C-sUAS activities. The JCO will lead and perform oversight of C-sUAS doctrine, requirements, materiel, and training standards and capabilities to establish joint solutions with a common architecture to address current and future emerging small UAS threats. It will coordinate development of joint operational concepts and joint doctrine for C-sUAS. It will lead coordination among the stakeholders to avoid duplication of effort and maximize efficiencies and effectiveness of program activities and any developmental efforts, accepting environmental and operational differences each service and agency faces. The JCO will lead development and coordination of common C-sUAS requirements, core training objectives, and policy. Activities in the other domains will be the responsibility of the individual services.

The JCO will establish and lead a General Officer Steering Committee which will have a representative assigned by each service and will include representatives from other departments/offices as designated in the DoDD. Working groups will initially be established for doctrine, training, policy, and materiel. The working groups will be led with O-6/GS-15 level personnel and composed of representatives of the services and other stakeholders. Working groups will address current and emerging threats, materiel requirements, policy issues, S&T, R&D, and doctrine and training. Coordination will be performed with all stakeholders.

The Director, Cost Assessment and Program Evaluation, with appropriate coordination, ensures that funds and resources required to support C-sUAS capabilities are included in the DoD Planning, Programming, Budgeting, and Execution process. The Secretaries of the Military Departments, in coordination with the EA, will appropriately fund C-sUAS programs across the Future Years Defense Program during the budget process to initiate research to explore and advance new and emergent C-sUAS technologies in alignment with this strategy, and appropriately fund any research and development C-sUAS capability when identified as the lead organization by the Joint Capabilities Integration and Development System or C-sUAS governance process. The EA plans, programs, and budgets for the research and development of UAS Groups 1, 2, and 3 C-sUAS capabilities with cost, funding, and expenses shared equitably among Military Services as appropriate to address DoD and Military Service C-sUAS requirements. The EA will identify enduring funding requirements to address joint C-sUAS capability needs.

ANNEX C. UNMANNED AIRCRAFT SYSTEM CATEGORIZATIONS

UA Category	Maximum Gross Takeoff Weight (lbs.)	Normal Operating Altitude (feet)	Speed (KIAS)
Group 1	0-20	< 1200 AGL	100 knots
Group 2	21-55	< 3500 AGL	< 250 knots
Group 3	< 1320	< 18,000 MSL	< 250 knots
Group 4	> 1320		Any Airspeed
Group 5	> 1320	> 18,000 MSL	Any Airspeed
Legend: AGL – above ground level; MSL – mean sea level; KIAS – knots indicated airspeed			

ANNEX D. REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces," June 13, 2005

Chairman of the Joint Chiefs of Staff Manual 5120.01A, "Joint Doctrine Development Process,"29 December 2014

Department of Defense, Artificial Intelligence Strategy, 2018

Department of Defense, National Defense Strategy, 2018

Deputy Secretary of Defense Policy Memorandum 16-003, "Interim Guidance for Countering Unmanned Aircraft," August 18, 2016

Deputy Secretary of Defense Policy Memorandum "Counter-Unmanned Aircraft Policy Memorandums," Tab A "Guidance for Employing Non-technical solutions for prevention and reducing the risk of unmanned aircraft incidents," May 7, 2020

Deputy Secretary of Defense Policy Memorandum "Counter-Unmanned Aircraft Policy Memorandums," Tab A "Guidance for Use of Counter-Unmanned Aircraft Technology Outside the United States to Protect DoD Personnel, Installations, Facilities, and Assets," May 7, 2020

Deputy Secretary of Defense Policy Memorandum "Counter-Unmanned Aircraft Policy Memorandums," Tab A "Risk-Based Assessment in Support of Counter-Unmanned Aircraft Activities to Protect DOD Facilities and Assets," May 7, 2020

Deputy Secretary of Defense Policy Memorandum 17-00X, "Supplemental Guidance for Countering Unmanned Aircraft," July 5, 2017

Deputy Secretary of Defense/Vice Chairman of the Joint Chiefs of Staff Memorandum, "Public-Private Partnerships Supporting the DoD Mission," April 25, 2013

DoD Directive 3800.01E, "DoD Executive Agent for Counter Small Unmanned Aircraft Systems for Unmanned Aircraft Groups 1, 2, and 3," February 21, 2020

DoD Directive 5101.01, "DoD Executive Agent," September 3, 2002, as amended

DoD Instruction 3224.03, "Physical Security Equipment (PSE) Research, Development, Test, and Evaluation (RDT&E)," October 1, 2007, as amended

DoD Instruction 5200.08, "Security of DoD Installations and Resources and the DoD Physical Security Review Board (PSRB)," December 10, 2005, as amended

ANNEX D. REFERENCES

Lt Col Jeffrey Lamport, COL (R) Anthony Scotto, "Countering the UAS Threat from a Joint Perspective," Joint Deployable Analysis Team, February 9, 2017

National Security Strategy, December 2017

National Strategy for Aviation Security of the United States of America, December 2018

Office of the Chairman of the Joint Chiefs of Staff, "DOD Dictionary of Military and Associated Terms," June 2020, as amended

Secretary of Defense Memorandum, "Designation of the Secretary of the Army as the DoD Executive Agent for Counter-Small Unmanned Aircraft Systems for Unmanned Aircraft Groups 1, 2, and 3," November 18, 2019

Senate Intelligence Committee, https://www.intelligence.senate.gov/hearings/open-hearing-worldwide-threats#, January 29, 2019

United States Code, Title 6, Section 1501

United States Code, Title 10, Section 130i

This Page Intentionally Left Blank