

AIR WAR COLLEGE

AIR UNIVERSITY

COUNTER-UAV SOLUTIONS
FOR THE JOINT FORCE

by

David J. Praisler, CDR, USNR

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: William Lewis

06 April 2017

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government, the Department of Defense, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.



Biography

CDR David Praisler is assigned to the Air War College, Air University, Maxwell AFB, AL. Commander Praisler graduated in 1997 from the United States Merchant Marine Academy in Kings Point, NY earning a Bachelor's of Science degree in Marine Engineering. After receiving his commission, he completed flight training earning his designation as a Naval Aviator in 1999.

His squadron assignments include Helicopter Combat Support Squadron THREE (HC-3), Helicopter Combat Support Squadron EIGHT (HC-8), Helicopter Training Squadron EIGHTEEN (HT-18), Helicopter Mine Countermeasures Squadron FOURTEEN (HM-14), and completed deployments onboard the USS DETROIT (AOE-4) and USS IWO JIMA (LHD-7) in support of Operation Enduring Freedom and Operation Iraqi Freedom. His was assigned to major staff duties at U.S. Fleet Forces Command in the Fleet Personnel Development and Allocation (N1) Directorate and most recently served as the Commanding Officer of Navy Operational Support Center Phoenix.

CDR Praisler has logged almost 3,000 mishap free flight hours in Navy aircraft including the T-34, TH-57, CH-46D and MH-53E. His awards include the Meritorious Service Medal, Navy and Marine Corps Commendation Medal (two awards), and Navy and Marine Corps Achievement Medal (two awards), as well as numerous unit awards.

Abstract

The recent commercial sales explosion of small, low cost UAV's has renewed discussions amongst security professionals and leaders at all levels of government concerning the threats presented by drones. For well over a decade, these concerns have been presented, discussed, admired, and assessed numerous times. However, a new urgency exists as negligent owners, criminals and terror organizations have realized the capabilities of these devices and are using them in deadly ways.

Small-UAV's, which include both remote controlled model aircraft and drones, have been on the commercial market for decades. However, they (specifically quadcopters or drones) have proliferated in staging numbers over the past few years driving renewed concerns and governmental regulations. While the sales figures are impressive, the capabilities of these devices to be used as surveillance and reconnaissance platforms as well as payload delivery vehicles are even more concerning. These capabilities when coupled with their inherent portability and an operator with evil intentions have proven to be deadly.

Fortunately, military and commercial organizations have searched for a means to deal with these small, slow, stealthy devices. Further, several systems have proven to be rather successful in defeating these small-UAV systems and have been employed at various civic and sporting events to monitor and deter potential threats from small-UAV's. As these counter-UAS systems have been developed and tested with success, the joint force must act quickly to choose an agile acquisitions model to procure and employ these weapons systems for the protection of property, assets and personnel. In complimentary fashion, the concept of operational employment of these weapons systems must also be agile and responsive to the evolving threat.

Introduction





The Air Force has maintained dominance of the air domain to such a degree that since Korean War, no American ground forces have been killed since 1953. However, American ground forces have new reasons to look up. The newest aerial threat, low cost commercially available remote controlled quadcopters (commonly referred to as drones), have stormed onto the world stage in huge numbers over the past several years and have the capacity to end air superiority in the future. The threat may be physically small and relatively inexpensive, however, their diminutive size, extensive capabilities and low cost make them extremely attractive for kids and criminals alike. Although this threat is not a new technology and has penetrated the discussions of military leadership for decades, the time for admiring the problem and forecasting trends needs to end quickly. The concern is such that the entire Joint Force must act quickly in order to protect its property, assets and people and uphold the record of success which began in 1953.

The small, very low cost, commercially available remote controlled quadcopter has proliferated at a frenzied pace over the past several years. The popularity of UAV's (unmanned aerial vehicle), commonly referred to as drones, has certainly attracted the attention of children, parents, commercial manufacturers, military and many levels of government. While UAV's have been a popular topic in military discussions and in the press lately, they have been in existence for quite some time. In fact, the first successful UAV flight occurred in England in 1917, whereas, the first remotely controlled model aircraft did not appear until the mid-1930's.

Although remotely controlled aircraft have been in existence for over 100 years, the language used to describe and classify these aircraft has lacked consistency much like the often confused terms of airplane and aircraft. The interchangeable labels used to describe these devices

often results in confusion over what kind of aircraft is being discussed. Possibly the most widely used term, and perhaps the most inaccurate is “drone.” The term, drone, became popular after the military began using large remotely piloted aircraft as targets for live fire exercises after WWII. After the Vietnam War, the Air Force began using the term RPV (remotely piloted vehicle). As the military often strives to renew its vocabulary periodically, in the 1990’s, the term UAV (unmanned aerial vehicle) came into vogue. The term UAS (unmanned aerial system) followed shortly to acknowledge that the aircraft itself was part of a larger system including a ground control element. Then, only a few years ago did the Air Force begin using the term RPA (remotely piloted aircraft) to ensure the human element of the system was not lost in the title.

Though many other less widely accepted terms have been used to some degree to describe these devices, the most widely accepted term is UAV when referring to the actual flying aircraft and UAS when referring to the system as a whole. As such, this paper will use these terms throughout. When discussing UAV’s, the spectrum of cost, size and range of capabilities is enormous therefore a simple three letter acronym will not suffice. While there is some diversity among organizations in regards to the classification of UAV’s, the FAA classifies UAV’s into two categories, small-UAV’s (.55-55lbs) and UAV (>55lbs). However, the Department of Defense has developed its own classification system, referenced below, and is the system of classification most appropriate for this discussion.

UAS Groups	Maximum Weight (lbs) (MGTOV)	Normal Operating Altitude (ft)	Speed (kts)	Representative UAS	
Group 1	0 – 20	<1200 AGL	100	Raven (RQ-11), WASP	
Group 2	21 – 55	<3500 AGL	< 250	ScanEagle	
Group 3	< 1320	< FL 180		Shadow (RQ-7B), Tier II / STUAS	
Group 4	>1320			Any Airspeed	Fire Scout (MQ-8B, RQ-8B), Predator (MQ-1A/B), Sky Warrior ERMP (MQ-1C)
Group 5		> FL 180	Reaper (MQ-9A), Global Hawk (RQ-4), BAMS (RQ-4N)		

Source: DoD Unmanned Aircraft System Airspace Integration Plan; V 2.0, 2011.¹

Thesis

The proliferation of small, highly capable, low cost unmanned aerial vehicles has developed into a significant threat to our installations, assets, and people. Because of this threat, the Joint Force should procure through short-term contracts proven counter-UAS systems for rapid and agile deployment based on asset criticality, vulnerability and threat level.



Current Threat Environment

“In the future, the Joint Force may confront heavily-armed violent extremists operating in the homeland armed with small drones and weapons delivery devices built with off-the-shelf components...” –Joint Operating Environment 2035²

The capabilities of low cost commercially available small-UAV's (group 1 and 2) has captured the attention of consumers of all types around the globe. The result has been an exponential growth of UAV sales in recent years and has generated serious safety concerns prompting the government to introduce operating regulations and ownership controls within the United States. Further, it is precisely because of these low cost capabilities that numerous government agencies including the Department of Homeland Security, the intelligence community, and all levels of the Department of Defense have taken notice and have expressed significant concern about the threats these devices present to the security of our joint force. Thus, the rampant proliferation of devices already in use and the significant increase in ownership forecast into the future drives the need for the acquisition of counter-UAS systems. Numbers alone however only address a portion of the concern. The capabilities of these devices at such a relatively low price point make them easy to obtain for recreational purposes or for use in nefarious ways.

Here, within the United States, the proliferation of small-UAV's has skyrocketed in only a few short years. In the FAA's Aerospace Forecast 2016-2035, they estimate personally owned UAV sales for 2016 reaching 1.9 million and increasing to 4.3 million units sold annually by 2020.³ Due to the unprecedented proliferation of these devices, in December of 2015, the FAA developed rules to mandate owner registration and regulate the operation of small-UAV's within the United States. In a speech on August 2nd, 2016, Michael Huerta cast some perspective on the proliferation of these devices. He stated that within the U. S., there are approximately 320,000








registered manned aircraft. Further, he stated that in only 8 months since the FAA's December 14th, 2015 implementation of UAV registration requirements, over 500,000 registrations had been filed.⁴ The rules, which are located in part 107 of the Federal Aviation Regulations, apply to all UAV's from .55lbs to less than 55lbs. Aircraft, including UAV's, weighing more than 55lbs are required to be registered using the existing Aircraft Registration Process. However, no requirement exists to register the smallest toy remote controlled UAV's. The regulations, implemented by the FAA, include UAV registration requirements, airspace operating limits, operator age restrictions and operator training requirements.

Although the sales figures are impressive, it is the inherent capabilities of these small-UAV's which really highlight their versatility in recreational use and unfortunately have demonstrated their effectiveness for destructive use. The economy of cost vs. capabilities could be expanded into a whole separate discussion and is the primary reason why these devices have grown in such popularity over such a short timeframe. Commercially available small-UAV systems for private use can cost anywhere from \$30 to \$3,000. These devices have a wide range of lifting capacities and speeds that are usually inversely proportional to their flight time. However, new improvements are being made every day which are generating drones that are cheaper, fly farther, remain airborne longer and carry more payload.

Since almost all low cost commercially available quadcopters have some sort of camera or video camera already installed on-board, the most obvious threat becomes ISR. These devices are often built around and include HD cameras and camcorders which turn them into cheap but reliable ISR assets. These purpose built aircraft can easily gather critical information about unit composition, pattern of life and troop movements. However, drones in this small-UAV category are not limited to carrying cheap cameras and GoPro action video recorders. The more

expensive, but more capable and still commercially available, heavy lift drones can easily tote high end 4k professional quality DSLR cameras as well. Additionally, FPV (first-person view) flight is a type of remote-control flying that has grown in popularity in recent years. FPV flight involves mounting a small video camera and television transmitter on an RC aircraft with an accompanying handheld video receiver-controller. Flight control beyond line of sight is accomplished by means of a live video down-link, commonly displayed on video goggles or a portable LCD screen or even a smartphone. When flying FPV, the pilot operates the aircraft based upon the video feed taken from the aircraft. As a result, FPV aircraft can be flown well beyond visual range, limited only by the range of the remote control and video transmitter.

Beyond the threat of adversary ISR, the payload carrying capacity of these devices becomes the ominous potential threat variable. Today, some of the most capable drones available on the commercial market can lift over 20lbs, remain airborne for over 40 minutes, exceed 85mph and are controllable at a range of up to 5km. The following chart identifies some of the most common commercially available drones on the market with a breakdown of their advertised range, lift capacity, speed and price. Though some of the drones listed on the chart do not advertise payload capacity beyond the manufacturer installed equipment, with just a small amount of ingenuity, even these smaller drones can be equipped to transport lightweight payloads. The chart highlights the fact that though these devices are small, the ISR capabilities, payload capacity, range and speed of the various devices can be quite significant.

Name	Image	Payload Capacity	Range (control)	Flight Time	Speed	Est. Price
DJI Phantom 4 ⁵ *Extremely popular, many versions available		Manufacturer installed 4k video camera	4.3 mi	30min	45mph	\$1,500 (DJI Phantom 3 retails for \$499)
Tarantula x6 ⁶ *Inexpensive beginner drone		Manufacturer Installed 2MP camera (GoPro capable)	100m	10min	n/a	\$55
Freefly Alta 8 ⁷ *Professional grade cinematography drone, GPS capable, folding chassis		20 lb Multi-adjustable load platform	Varies based upon choice of controller	35 min ~10 min w/20lb load	35mph	\$17,000
Teal Drone ⁸ *FPV racing drone		FPV camera only	~1 mi	20 min	85mph	\$1300
DJI Mavic ⁹ *Foldable to 3.5"x3.5"x8"		Manufacturer installed 4k video camera	4.3 mi	30 min	40mph	\$1000
DJI Agras ¹⁰ *Professional quality agriculture crop spraying		10 Liters of liquid ~22 lbs	.6 mi	24 min ~10 min with full tank load	50 mph	\$12,000
Fastest RC Model Aircraft ¹¹ *Only posted to show to speed and stealth capabilities		n/a	n/a	n/a	440mph	n/a

A secondary but no less important consideration is the issue of portability. The diminutive size of these devices, such as the DJI Mavic in the preceding chart, allow for easy hand carry or backpack transport. With the combination of portability and rapid deployment capability, these systems can overcome their relatively short ranges and launch at very close-in range to their intended target area. While potentially increasing the operators' risk of detection, launching the drone in close proximity to the target area severely reduces the time available for friendly forces to detect and act upon the threat.

Espousing potential threats based upon system capabilities serves only as a starting point for discussion, actual documented use tells the real story. Several instances of criminal activity in recent years have made headlines and have generated public safety concerns. The concern is not without good reason. There are numerous examples within the U.S. where small-UAV's have been used in hazardous, criminal and suspicious ways. For example, former Northeastern University student Rezwan Ferdaus, is currently serving 17 years in prison for plotting to fly F-4 and F-86 model aircraft loaded with C-4 into the Pentagon and U.S. Capitol building.¹² In another example, on January 26, 2016, a popular version of the DJI Phantom quadcopter crashed into a tree on the White House grounds.¹³ In addition to examples such as these, the FAA documents over 100 cases a month (and growing), where UAV's have been sighted in near miss situations at airports around the nation.¹⁴

Beyond U.S. borders, criminals and terrorists alike have significantly increased their use of drones to conduct ISR or deliver kinetic munitions against friendly forces. In a relatively high profile case, on April 22, 2016, a drone carrying radioactive sand landed on the roof of Japanese Prime Minister, Shino Abe's residence.¹⁵ More concerning are recent reports which have confirmed that ISIS successfully conducted direct attacks using small munitions using these devices in Mosul. Military officials in theater have confirmed the use of small grenade like ammunition dropped from small commercially available drones.¹⁶ In addition, although not criminally oriented, China uses drones in this category equipped with flame throwers for the purposes of burning trash hung up on high voltage transmission lines.¹⁷ These events are just a small snapshot of how an enemy is currently using or might intend to use small UAV's. Thus, the threat is very real. The evolution from ISR to kinetic threat from hostile UAV's is happening now. While the ISR threat will continue in ever stealthy ways to include using micro

technologies, the use of small-UAV's for the transport and delivery of kinetic payloads is only going to multiply over time. The worldwide proliferation of this technology coupled with capabilities limited only by the enemy's imagination make UAV's the air threat of today.

Current Counter-UAS Capabilities

With the spotlight shining brightly onto the threats posed by small UAV's, the race to develop and procure technologies to counter the UAV threat has garnered the attention of both the military and commercial industry. The efforts to counter the UAV threat have generated much in innovation and system development in just a short time. Though numerous companies have emerged and have developed their own unique methodologies to defeat the UAV threat, in general, there is a basic formula to the operation of counter-UAV systems. First however, it is important to recognize that defeating any part of the UAV system including the operator, the ground control station, the electromagnetic control signal, or the UAV itself, results in the defeat of the threat. As such, since these countermeasures take a systems level approach to defeating the UAV threat, the most appropriate naming convention for these platforms is counter-UAS. Though there are differences among manufacturers as to how each step is accomplished, the first step towards defeating the UAV threat must be to find or detect the UAV. The system then must be able to track and identify the UAV and, if appropriate, defeat the UAV. A brief discussion of these steps follows along with some examples of how these steps are accomplished.

Detecting small-UAV's is perhaps the most difficult part of the c-UAS kill chain. Detection, whether through radar, acoustic, optical or IR surveillance is problematic given the small stealthy size of these devices. Exacerbating this are environments such as airports and urban areas where the electromagnetic spectrum becomes extremely crowded and creates a

significant discrimination problem.¹⁸ In addition to this difficulty, because the UAV may be launched at close range to the target, the relatively short range and flight duration of small-UAV's significantly decreases the time available to observe and detect the UAV. The weakness of short flight distances is mitigated by the small devices portability which, in turn, compounds the defensive problem set. Hidden in a backpack and transported to a nearby location presents a significant challenge for detection of the UAV. However, it potentially opens up an area of weakness by increasing the potential for exposing an operator to detection by security forces.

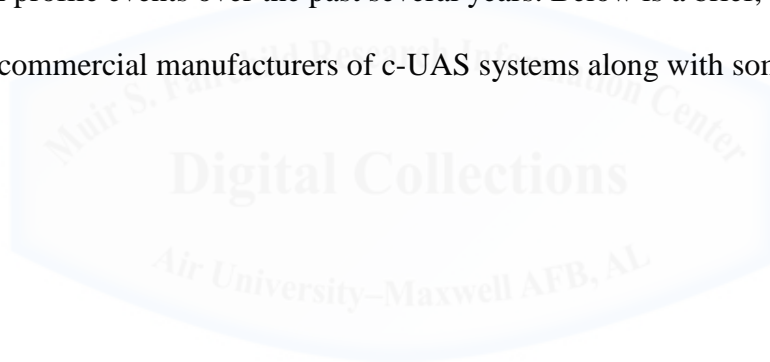
Once the C-UAS system detects the UAV, the system must be able to track and identify the UAV and be able to discriminate it from other airborne objects like birds, flying debris or other aircraft. In the case of Lockheed's Icarus, the sensors, which detect the UAV threat, feed important information to a database where radio-frequency, acoustic and imagery signatures are stored. The system then evaluates and compares this information to make a determination on what type of UAV is being tracked.¹⁹ One manufacturer, Dedrone, calls this type of information drone DNA.²⁰

The final step in the kill chain of a counter-UAS system is Defeat. Of course, only the system developer's imagination and the amount of acceptable complexity limits the range of options for defeating a UAV. Successful destructive defeat methods have ranged from shotguns to .50 caliber machine guns to hellfire missiles or even high energy lasers. Other defeat options have included the use of eagles to attack and disable the drone, or by using a drone, carrying a net, to drop the net onto the adversary device. On the other end of the spectrum, non-destructive or non-lethal defeat methods are generally more sophisticated and are preferable in almost all environments. The non-lethal approach has several advantages the first being system employment in any environment, especially urban areas. Non-lethal defeat mechanisms result in

zero collateral damage which results in limited if any risk of casualties while also allowing friendly forces to recover the device and gather intelligence on the adversary.

However, non-kinetic defeat solutions may not always work. Most commercially available systems utilize some form of direct line of sight RF communications or GPS signal for guidance. However, small home built systems could incorporate inertial navigation components which would negate the requirement for a communication link. Should this be the case, non-kinetic defeat through the use of electromagnetic frequency jamming would prove ineffective.²¹

Although c-UAS systems are not new, the discussion on c-UAS systems began almost a decade ago. Since that time, numerous c-UAS systems have been developed and successfully employed at high profile events over the past several years. Below is a brief, certainly not all-inclusive, list of commercial manufacturers of c-UAS systems along with some details of their system.



Current off the shelf systems

c-UAS Platform	Manufacturers description
Dedrone ²²	<p>Dedrone provides an automatic, integrated and self-contained drone detection, identification and counter-measure platform to detect drone threats and their operators 24/7. DroneTracker is the only modular system on the market that can be customized to address site-specific threats, adapted for easy integration to an existing security program, and accommodates unique building structures, landscapes and other exterior conditions.</p>
CACI SkyTracker ²³	<p>CACI's SkyTracker unmanned aircraft systems (UAS) solution is a new, precision system to protect high-value assets and support public safety against the escalating threat posed by the inadvertent or unlawful misuse of UAS.</p> <p>The SkyTracker system accurately and reliably detects, identifies, and tracks UAS threats. This proprietary CACI technology has been demonstrated to address a variety of UAS threat scenarios. The system is widely applicable, from protecting airports to safeguarding critical infrastructure or events – anywhere UAS pose a potential risk to people or assets. SkyTracker provides continuous, automated monitoring, day or night, in any weather condition. This system has the unique capability to identify and locate both the UAS and its ground operator, improving responders' ability to act in incidents of inadvertent or unlawful misuse.</p> <p>Unlike other technologies, SkyTracker provides passive detection that does not interfere with legitimate electronics or communications systems in the area, or with UAS that are being operated responsibly as determined by the U.S. government.</p>
Liteye Systems ²⁴	<p>AUDS is designed to disrupt and neutralize Unmanned Aerial Vehicles (UAVs) engaged in Hostile Airborne Surveillance and potentially Malicious Activity. The AUDS system combines electronic scanning radar target detection & classification, Electro Optic (EO) tracking and directional RF inhibition capability over three independent RF bands.</p> <p>AUDS is a smart-sensor and effector package capable of remotely detecting small UAS and then tracking and classifying them before providing the option to disrupt their activity. The system may be used in remote or urban areas to prevent UASs being used for terrorist attacks, espionage or other malicious activities against sites with critical infrastructure. AUDS not only works to cover your airspace, but also as a ground surveillance system as well.</p>
Battelle DroneDefender ²⁵	<p>Battelle DroneDefender systems are non-kinetic cUAS solutions developed to instantaneously defend airspace against commercial drones without compromising safety or risking collateral damage.</p> <p>Traditional defense mechanisms against small UAS, such as shooting them down, pose safety risks in many situations.</p> <p>DroneDefender is a directed-energy unmanned aircraft system (UAS) countermeasure. It quickly disrupts the adversary's control of the drone, neutralizing it so that no remote action, including detonation, can occur, minimizing drone damage and risk to public safety.</p>
Selex-ES Falcon Shield ²⁶	<p>The rapid proliferation of micro/mini UAVs, also known as drones, is recognized globally as a growing potential threat to national and commercial security. Easy to make, cheap to buy, simple to fly and hard to detect, commercially available drones are one of the most quickly evolving technological threats to both military and civilian environments. In response to this threat, Finmeccanica – Selex ES has introduced Falcon Shield, which can provide users with a rapidly deployable, scalable and modular system to detect, disrupt, deny and defeat the potential threat.</p> <p>Falcon Shield provides users with a multi-spectral sensing capability and, uniquely through the integration of an electronic attack capability, a multi-layered threat response. Falcon Shield is derived from Selex ES's heritage associated with the provision of short-range defense solutions against a variety of airborne threats.</p> <p>Falcon Shield exploits Selex ES's high-performance, passive Electronic Surveillance and Electro-Optical sensors, combined with scenario-specific radar to provide a fully integrated threat detection, identification and tracking capability that is able to operate in environments ranging from wide area through to high-clutter, 'urban canyons'.</p>

Joint Force c-UAS system selection

Thus far, I have described the threat and have investigated some of the many systems, which are either in development or have already been employed to counter this threat. Now the question is, what counter-UAS system technology does the joint force invest in and how should it do that? If the wisdom contained with the CJCS Joint Operating Environment 2035 teaches us anything, it is to look for solutions beyond the current threat. While purchasing and implementing currently developed and tested equipment may solve today's threat, tomorrow's technology is, in some ways, already here. However, the joint force cannot ignore this rapidly progressing threat which will not wait for a prolonged c-UAS system development timeline. With the proliferation of extremely low cost and expendable drones, the joint force must field and employ c-UAS systems now. But what system does the Air Force choose? The answer may come from events such as JIAMDOD's Black Dart and the FAA's Pathfinder program.

Black Dart, "is an annual US military joint exercise where vendors demonstrate their latest countermeasures against enemy drones, ranging from jamming their signal source; taking direct control of them; shooting them down with high powered lasers and ground to air missiles; and deploying counter-drones designed to conduct air to air combat missions."²⁷ A yearly event which began in 2002 under the direction of the Defense Intelligence Agency, Black Dart started out as a UAS capabilities demonstration and development exercise. Run under the control of USNORTHCOM from 2006 to 2010, now JIAMDOD (Joint Integrated Air and Missile Defense Organization) controls this event. Since 2010, the annual Black Dart exercise has evolved into a counter-UAS technology demonstration, test and evaluation exercise. A classified event until 2014, the event has attracted an increasing amount of participants each year. Due to an expanding threat spurred by proliferation over the past several years, the event focuses on

technologies for countering small-UAV's. During Black Dart 2016 for example, fifty-five different systems were tested against varying targets.²⁸ This level of collaboration and competition has proved to be highly successful and should be the proving grounds for selecting an acceptable counter-UAS system.

However, Black Dart is not the only proof of concept exercise conducted to demonstrate the capabilities of counter-UAS systems. Under its Pathfinder program, the FAA in partnership with the Department of Homeland Security works with companies to observe and evaluate counter-UAS system effectiveness while ensuring non-interference with normal airport operations.²⁹ For example, in February 2016, the FAA invited CACI International to test its SkyTracker detection system at Atlantic City Airport. For over a week, this system was tested in 141 operations against small-UAV's and was able to triangulate on the signals and locate both the UAV and the operator.³⁰ The existence and conduct of these test, evaluation and demonstration exercises should not obscure the fact that several manufactures have already employed fully operational c-UAS systems to monitor and protect high profile civic and sporting events.

In the end however, a fully matured, tested and successfully deployed c-UAS system may not be the final choice of the joint force. One of the many lessons learned from the Black Dart exercises is that currently fielded equipment may be adapted to fulfil c-UAS requirements. According to Air Force Maj Scott Gregg, lead coordinator for Black Dart 2016, "ultimately, there is no "Silver Bullet" counter-UAS system that will solve the UAS problem. It will take a multitude of systems working together to mitigate the threat."³¹ Additionally, he goes on to say, "many of the systems that have participated in Black Dart over the years are currently fielded programs of record, currently fielded systems that were never designed for counter-UAS because

at the time they were designed, UAS wasn't really a threat.”³² These comments suggest two things. First, the chosen solution does not have to be the newest and most exquisite technology available. Second, through internal adaptation, innovation and open competition, only the most capable systems should be chosen based off of demonstrated capabilities. Thus, the effectiveness of the system should inform the c-UAS system choice, preferably through the successful demonstration of the system at JIAMDO's Black Dart.

c-UAS system employment CONOPS

*“To meet the challenges of the operational problem, the future Joint Force must be: distributable, resilient, and tailorable, as well as employed in sufficient scale and for ample duration.” - JAM-GC, a New Joint Operational Concept*³³

Following guidance contained within documents such as CCJO v3.0 and JOE 2035, strategic agility should underpin the basic operating concept for counter-UAS system employment. Knowing full well that, “military success in the future rarely will be the product of radically new ideas,”³⁴ this concept will no doubt require modification as the threat evolves and lessons are learned. Regardless, as a starting point, the procurement and employment of c-UAS systems should support the fundamental purposes of deterrence and denial in a wide range of operating environments. To meet these purposes, the objective of c-UAS operations should be security through deterrence and denial by responsive and rapidly distributable systems in support of worldwide demands.

Counter-UAS systems should be employed force wide as a new means for security forces to maintain control and safety over critical assets. As such, these systems should be considered a new tool for security professionals to use for the safety and protection of people, property and resources. Stated another way, security forces can use c-UAS systems as a tool for deterring or disrupting any possible planning, ISR, or active operations by potential terrorists and criminals against our facilities or people. Whether these systems are used for long term UAV surveillance and defeat, or used in short term rapid response applications, the system can be a valuable tool for deterring adversaries from employing UAV's and placing our assets at risk. Employment of c-UAS systems and the accompanying authorities and responsibilities should be nested within the existing governance for anti-terrorism and force protection.

To interrupt predictability and hence reduce vulnerability, c-UAS systems should be acquired in sufficient numbers so as to fulfil support requirements derived by asset criticality, vulnerability and threat assessments. This does not suggest all identified requirements are satisfied on a full time basis. Again, the key tenant is strategic agility. For agility, these systems should be rapidly deployable in support of HVU (high value unit) security requirements, intelligence based threats, installation RAM's (random anti-terrorism measures) and in limited cases where high priority threat assessments mandate an enduring requirement. As an example, during restricted maneuvering events when an HVU asset such as an aircraft carrier is transiting into and out of port, a portable c-UAS system can be on loaded via MH-53E Sea Dragon or C-2 Greyhound. The system is set-up, operated and maintained by contractor support with command, control and response authority owned by the ship's captain. When the event is complete, the system is off-loaded and made available for use at another location.

This type of temporary deployment, operation, and re-deployment construct, which can be used in almost any situation and any environment, drives system development and acquisition in three significant ways. First, this construct requires a system that is relatively compact, lightweight and portable. Placement of c-UAS systems can range from the deck of an aircraft carrier to an austere operating area accessible only by four wheel drive vehicles. Second, the distributed operations concept does not require large quantities of systems employed worldwide. The demand signal, whether derived by intelligence or forecasted RAM's, should drive the requirement for capacity. Here, flexibility or tailorable response is a guiding principle. Third, the wide range of threat and deployed environments demand a wide range of system capabilities. For example, defeat options in urban environments within the United States are significantly different than the options available to a forward operating base in an austere OCONUS location where potentials for property damage and civilian casualties are remote.

The services should field the most fully developed system in low quantities. Because of rapid advances in technology, the services should compete for contract on a very short term basis. The service should not seek ownership of these systems which may prove to become obsolete as advancements in technology occur. Additionally, the threat may not prove to become as rampant as forecasted. Further, lessons learned based on chosen operating concepts may lead to significant changes in system requirements and the numbers of systems to be fielded. Since it is likely that UAS technology will continue to mature over time, the joint force should only award short term end-to-end support contracts to the developer who produces the system that proves most effective as demonstrated at the annual Black Dart exercises.

c-UAS system Acquisition in support of CONOPS

Once, a system is chosen to provide counter-UAS protection based on demonstrated success, the next question is how should the joint force procure a counter-UAS weapon system. What system is chosen and how the services intend to employ the system informs the methodology of procurement. If the system is an already fielded program of record that can be adapted to satisfy the c-UAS mission, the procurement question may be nil or may drive some type of contract modification. If the choice is an off-the-shelf commercially available system the procurement and system employment calculus fundamentally changes. The joint force does not need to become wedded to these systems only for them to rapidly become obsolete and end up gathering dust in an old warehouse. Because technology is evolving at such a rapid pace which complicates the logistics of maintenance and manpower, the joint force should field a c-UAS system via a short term fully supported contract.

Like many other technologies, counter-UAS technology is not static. On the contrary, as the exercises conducted at Black Dart can attest, this technology is evolving at a rapid pace. However, that does not mean we can afford to wait on the procurement of a fully developed c-UAS system. Nor does it mean we need to rush out and become tied to a technological prototype only to be shackled to its future development. In regards to the acquisition of fleeting technologies, during a public briefing, Lt Gen Kwast, Commander, USAF Air University, commented on the short temporal nature of today's technological advantages saying, "In the industrial age, the technological edge lasted years and sometimes decades. Then, the military could procure a weapons system and expect to utilize that system for a long time. The speed of technology has simply outpaced this type of acquisitions model."³⁵

Some may still contend that ownership of weapons systems and intellectual rights is still the right way to go. They point to spiral development of technologies to adapt existing programs of record to stay current and on the technological leading edge. However, spiral development of rapidly evolving technologies can bring second order logistical problems like standardization and compatibility as each modification breeds different system configurations. Lessons can be learned from the acquisitions of other rapidly developing technologies like the Predator and Global Hawk where standardization has complicated logistics and maintenance because of differences in systems configurations.³⁶

Rapid acquisitions processes do not allow sufficient time to develop technical data and integrate training requirements. As espoused in the RAND study, “Building – and retaining – a well-trained cadre of Air Force personnel for maintaining future Predators has proven to be a challenge, even in peacetime.”³⁷ The complexity of the system and the one-off hand-built component make up in some ways exacerbates this challenge. Given these challenges, it becomes clear that organic capabilities will not be readily available to employ the weapons system. Further, initial training development could take several years. With manpower already stretched beyond the comfort of most manpower analysts and commanders, siphoning additional manpower assets from other platforms is unacceptable.

Traditional acquisitions processes, where a system is designed and fielded based on certain requirements, that come with prolonged testing and production lines and involve long term maintenance and modernization plans are simply not agile enough to address the threat now and evolve rapidly as technology advances into the future. The potential for rapid technological evolution, resulting in a high turnover of system configurations, further exacerbates the assessment of maintenance requirements and the determination of repair level assignments. The

problem grows even larger when support and test equipment must be designed and fielded as well, while ensuring system compatibility. Thus, the sustainment costs tend to grow quite large even though the number of systems may be relatively small. While only a full cost-benefit analysis would tell the full story, lessons and estimates can be drawn from other Contract vs Organic Support cost examinations such as the RAND study on End-to-End UAV Support Considerations.

Thus, the need to rapidly field a system takes priority over developing the most universally capable system that meets all current and forecast requirements. A Contractor Supplied Logistics model would complement an operating concept grounded in rapid and tailored response, thereby achieving maximum strategic agility. As lessons are learned, technological advances are realized, and CONOPS are changed, the counter-UAS system that proves to be most agile and effective should be chosen to mitigate the threat. Short term contracts that provide support on an as needed rapidly deployable basis may prove to be the best method for fielding the most technologically advanced and agile counter-UAS capability. Also, short term contracts which compete often tend to drive costs down while avoiding complex organic training and maintenance requirements. As UAS technology develops and adversary tactics evolve, only the systems that remain on the leading edge of UAS detection and defeat should be awarded contracts to provide systems going forward.

Conclusion

The joint force has pondered, discussed, and forecast the threat possibilities posed by small-UAV's for too long. Criminals and terrorists have used and will continue to use these low cost, commercially available and disposable devices in ever creative ways to threaten our personnel, assets and even innocent civilians. The time for admiring the problem must reach an end. The joint force has researched, tested and successfully demonstrated the ability of counter-UAS weapons systems which can deter and defeat these serial threats and now must choose and employ that system today. In doing so, the joint force should deploy and redeploy these systems with strategic agility and couple that operational approach with an equally agile acquisitions plan that periodically competes the contract for providing the most technologically advanced systems available as the threat continues to evolve. The threat is here and cannot be allowed to put our assets and personnel at risk; the capabilities are available; the methodology is sound; it is time to act.

Notes

¹ Department of Defense, *Unmanned Aircraft System Airspace Integration Plan*, (March 2011), Appendix D-3.

² Joint Chiefs of Staff, *Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World*, (July 2016), 27.

³ Federal Aviation Administration, *FAA Aerospace Forecast: Fiscal Years 2016-2036*, (March 2016), 31.

⁴ Michael Huerta, "White House Drone Day," (Speech presented in Washington, DC on August 02, 2016), transcript available at: https://www.faa.gov/news/speeches/news_story.cfm?newsId=20594&omniRss=speechesAoc&cid=104_Speeches.

⁵ DJI Phantom 4 Pro Specifications, accessed April 01, 2017, <http://www.dji.com/phantom-4-pro/info#specs>.

⁶ Tarantula X6 Specifications, accessed April 01, 2017, <http://www.dronesglobe.com/affordable-list/under100/>.

⁷ Free Fly Alta 8 Specifications, accessed April 01, 2017, <http://freeflysystems.com/alta-8/specs>.

⁸ Teal FPV Drone Specifications, accessed April 01, 2017, <https://tealdrones.com/tech-specs/>.

⁹ DJI Mavic Specifications, accessed April 01, 2017 <http://www.dji.com/mavic/info#specs>.

¹⁰ DJI Agras MG-1 Specifications, accessed April 01, 2017, <http://www.dji.com/mg-1/info#specs>.

¹¹ World's Fastest RC Jet, accessed April 01, 2017, <https://throt-l.com/aircraft/the-worlds-fastest-remote-controlled-jet-is-halfway-to-the-sound-barrier-at-440-mph/>.

¹² Richard Whittle, "Military Exercise Black Dart to tackle nightmare drone scenario," *New York Post*, (July 25, 2015), accessed September 20, 2016, <http://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/>.

¹³ Joe Charlaff, "Hostile UAV's...And The Defenses Against Them," *Homeland Security Today*, (September 08, 2015), accessed September 20, 2016, <http://www.hstoday.us/single-article/analysis-hostile-uavs-and-the-defenses-against-them/50fd208f81aa7e50c412bd3458cecb2d.html>

¹⁴ Federal Aviation Administration, "UAS Sightings Report," accessed 17 March 2017, https://www.faa.gov/uas/resources/uas_sightings_report/.

¹⁵ Charlaff, "Hostile UAV's....And The Defenses Against Them."

¹⁶ Jeff Schogol, "ISIS Using Small Drones to Drop Bombs on Iraqis," *Military Times*, (January 11, 2017), accessed February 21, 2017, <http://www.militarytimes.com/articles/isis-using-armed-drones>.

¹⁷ Peter Farquhar, "China is Using a Flamethrowing Drone to Clean Rubbish off Power Lines," *Business Insider*, (February 20, 2017), accessed February 21, 2017, <http://www.businessinsider.com/china-is-using-a-flamethrowing-drone-to-clean-rubbish-off-power-lines-2017-2?r=UK&IR=T>.

¹⁸ Massimo Annati, "Counter-Unmanned Aerial Vehicle Technologies," *Military Technology*, (Vol 40, no.5, May 2016), 24.

- ¹⁹ Yasmin Tadjdeh, "Defense Industry Developing Systems to Defeat Enemy Drones," *National Defense*, (Vol 100, no.746, January 2016), 22.
- ²⁰ Dedrone Website, accessed April 02, 2017, <http://www.dedrone.com/en/dronetracker/drone-protection-software>.
- ²¹ Tadjdeh, "Defense Industry Developing Systems to Defeat Enemy Drones," 22.
- ²² Dedrone Website, accessed April 02, 2017, <http://www.dedrone.com/en/dronetracker/drone-protection-software>.
- ²³ CACI Website, accessed April 02, 2017, <http://www.caci.com/Skytracker/>.
- ²⁴ Liteye Website, accessed April 02, 2017, <http://liteye.com/counter-uas.html>.
- ²⁵ Battelle Website, accessed April 02, 2017, <https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS-technologies/dronedefender>.
- ²⁶ Selex-ES Website, accessed April 02, 2017, <http://www.us.selex-es.com/-/falconshield>.
- ²⁷ Charlaff, "Hostile UAV's....And The Defenses Against Them."
- ²⁸ Yasmin Tadjdeh. "Inside Black Dart: How the Military Prepares for a Future Drone War," *National Defense*, (Vol 100, no.742, September 2015), 34.
- ²⁹ Graham Warwick, "FAA, DHS To Test Three More Counter-UAV Systems," *The Weekly of Business Aviation*, (Vol 101, no.19, May 16, 2016), 7.
- ³⁰ Ibid., 7.
- ³¹ Tadjdeh, "Inside Black Dart: How the Military Prepares for a Future Drone War," 37.
- ³² Ibid., 36.
- ³³ Michael Hutchens, et al., "JAM-GC, a New Joint Operational Concept: Built on the Air-Sea Battle Chassis," as submitted to Joint Forces Quarterly for publication, (January 2017), 8.
- ³⁴ Department of Defense, *Capstone Concept for Joint Operations V3.0*, (January 2009), iv.
- ³⁵ Stephen L. Kwast, Lieutenant General (USAF), "Innovation through DoD Collaboration with Civilian Academia and Business," Keynote Speech, (Futures Lab, Auburn Montgomery Campus), January 20, 2017.
- ³⁶ John G. Drew, et al., *Unmanned Aerial Vehicle End-to-End Support Considerations*, (Santa Monica, CA: Rand, 2005), 53.
- ³⁷ Ibid., 41.

Bibliography

References: Articles

Annati, Massimo. "Counter-Unmanned Aerial Vehicle Technologies." *Military Technology*. Vol 40, no.5. (May 2016): 24-27.

Charlaff, Joe. "Hostile UAV's....And The Defenses Against Them." *Homeland Security Today*, September 08, 2015. Accessed September 20, 2016. <http://www.hstoday.us/single-article/analysis-hostile-uavs-and-the-defenses-against-them/50fd208f81aa7e50c412bd3458cecb2d.html>

Farquhar, Peter. "China is Using a Flamethrowing Drone to Clean Rubbish off Power Lines." *Business Insider*. February 20, 2017. Accessed February 21, 2017. <http://www.businessinsider.com/china-is-using-a-flamethrowing-drone-to-clean-rubbish-off-power-lines-2017-2?r=UK&IR=T>.

Host, Pat. "Army's Solid State Laser Testbed Successfully Destroys UAV In Test." *Defense Daily*. June 07, 2013.

Hutchens, Michael (USN); Dries, William (USAF); Perdew, Jason (USMC); Bryant, Vincent (USA); Moores, Kerry (JS J-7). *JAM-GC, A New Joint Operational Concept: Built on the Air-Sea Battle Chassis*. As Submitted to Joint Forces Quarterly for publication. January 2017.

Knowles, John. "Going Small: Jamming the Mini-Drones." *Journal of Electronic Defense*. Vol 38, no.10. (October 2015): 26-30.

Lamport, Jeffery; Scotto, Anthony. "Military Must Prepare for Unmanned Aircraft Threat." *National Defense*. Vol 101, no.753. (August 2016): 22.

Mehta, Aaron. "History Tuesday: The Origin of the term Drone." *Defense News*. May 14, 2013. (Blog?)

Roosevelt, Ann. "Schafer Corp. Moves Toward Applying Technology For Fielded Systems." *Defense Daily*. September 25, 2014.

Schogol, Jeff. "ISIS Using Small Drones to Drop Bombs on Iraqis." *Military Times*. January 11, 2017. Accessed February 21, 2017. <http://www.militarytimes.com/articles/isis-using-armed-drones>.

Sirak, Michael. "ATK Unveils Counter UAV Systems As Part Of Growing Portfolio." *Defense Daily*. August 21, 2007.

Tadjdeh, Yasmin. "Defense Industry Developing Systems to Defeat Enemy Drones." *National Defense*. Vol 100, no.746. (January 2016): 22-23.

Tadjdeh, Yasmin. "Inside Black Dart: How the Military Prepares for a Future Drone War." *National Defense*. Vol 100, no.742. (September 2015): 34-37.

Warwick, Graham. "FAA, DHS To Test Three More Counter-UAV Systems." *The Weekly of Buisness Aviation*. Vol 101, no.19. (May 16, 2016): 7.

White, Andrew. "Mini- and Micro Unmanned Aerial Vehicles (UAV)." *Military Technology*. Vol 39, no.7/8. (Summer 2015): 46-49.

Whittle, Richard. "Counter-Drone Exercise Black Dart Expands, Moves to Eglin AFB." *Breaking Defense*. September 02, 2016. Accessed January 26, 2017. <http://breakingdefense.com/tag/black-dart/>.

Whittle, Richard. "Military Exercise Black Dart to tackle nightmare drone scenario." *New York Post*. July 25, 2015. Accessed September 20, 2016. <http://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/>.

References: Books

Drew, John G.; Shaver, Russell; Lynch, Kristin F.; Amouzegar, Mahyar A.; Snyder, Don. "Unmanned Aerial Vehicle End-to-End Support Considerations." Santa Monica, CA: Rand, 2005.

Ehrhard, Thomas P., "Air Force UAV's: The Secret History." Mitchell Institute Study, July 2010.

Zaloga, Steven J., and Palmer, Ian. "Unmanned Aerial Vehicles: Robotic Air Warfare 1917-2007." Oxford: Osprey, 2008.

References: DOD pubs

Federal Aviation Administration. "FAA Aerospace Forecast: Fiscal Years 2016-2036." March 2016.

United States, Department of Defense. "Capstone Concept for Joint Operations V 3.0." January 2009.

United States, Department of Defense. "Unmanned Aircraft System Airspace Integration Plan." March 2011.

United States, Joint Chiefs of Staff. "Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World." July 2016.

United States, Office of the Secretary of the Air Force. “*Air Force Future Operating Concept: A View of the Air Force in 2035.*” September 2015.

References: Websites

DJI Phantom 4 Pro Specifications. Accessed April 01, 2017.
<http://www.dji.com/phantom-4-pro/info#specs>.

Tarantula X6 Specifications. Accessed April 01, 2017.
<http://www.dronesglobe.com/affordable-list/under100/>.

Free Fly Alta 8 Specifications. Accessed April 01, 2017. <http://freeflysystems.com/alta-8/specs>.

Teal FPV Drone Specifications. Accessed April 01, 2017. <https://tealdrones.com/tech-specs/>.

DJI Mavic Specifications. Accessed April 01, 2017.
<http://www.dji.com/mavic/info#specs>.

DJI Agras MG-1 Specifications. Accessed April 01, 2017. <http://www.dji.com/mg-1/info#specs>.

World’s Fastest RC Jet. Accessed April 01, 2017. <https://throt-l.com/aircraft/the-worlds-fastest-remote-controlled-jet-is-halfway-to-the-sound-barrier-at-440-mph/>.

Federal Aviation Administration. “UAS Sightings Report.” Accessed March 17, 2017.
https://www.faa.gov/uas/resources/uas_sightings_report/.

Dedrone Website. Accessed April 02, 2017.
<http://www.dedrone.com/en/dronetracker/drone-protection-software>.

CACI Website. Accessed April 02, 2017. <http://www.caci.com/Skytracker/>.

Liteye Website. Accessed April 02, 2017. <http://liteye.com/counter-uas.html>.

Battelle Website. Accessed April 02, 2017. <https://www.battelle.org/government-offerings/national-security/aerospace-systems/counter-UAS-technologies/dronedefender>.

Selex-ES Website. Accessed April 02, 2017. <http://www.us.selex-es.com/-/falconshield>.

Reference: Speech

Huerta, Michael, “White House Drone Day.” Speech presented in Washington, DC on August 02, 2016. Transcript available at:
https://www.faa.gov/news/speeches/news_story.cfm?newsId=20594&omniRss=speechesAoc&cid=104_Speeches.

Kwast, Stephen L., “Innovation through DoD Collaboration with Civilian Academia and Business.” Keynote Speech. Futures Lab, Auburn Montgomery Campus. January 20, 2017.

