Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority

Lt Col Thomas S. Palmer, USAF
Dr. John P. Geis II, Colonel, USAF, Retired

Introduction

The year is 20XX, and after breakdowns in diplomatic and economic efforts to solve an international crisis, the US Air Force (USAF) has been tasked to lead major combat operations to destroy a hostile country's strategic targets. After weeks of nonstop preparations, planning, and coordination at a hometown USAF base, the first wave of 12 F-22 stealth fighters and two KC-10 aerial refueling tankers are just two hours from starting engines to begin their transoceanic flight.

Without any warning, several small black specks appear on the horizon and quickly head directly for the fighters. As the black specks get closer, they are visually identified by a crew chief as medium-sized civilian quadcopters carrying several small objects. The lead quadcopter drops a Thermite grenade explosive onto the first fighter causing a fuel tank rupture and massive fire. Next, another quadcopter attacks the last fighter in the parking row causing it to burst into flames, blocking any escape for the other 10 aircraft. Five more quadcopters arrive onto the scene, destroy the remaining fighters and then the two KC-10 tankers, killing 20 personnel and injuring 30 more in the resulting catastrophic fires.

As rescue personnel scramble to save lives, 10 more quadcopters swarm the airfield and destroy 20 more aircraft as well as the air base's enormous fuel storage tanks. Almost the entire fighter wing's fleet of fifth-generation fighters, worth billions of dollars, is incinerated. No one knows who controlled the quadcopters, and there was nothing anyone on the airfield could do to stop the onslaught of attacks, or was there? Although this is a fictitious scenario, the technologies to create such a disaster exist today.[1]

Unmanned aerial systems (UAS), also known as "drones," unmanned aerial vehicles (UAV), and remotely piloted aircraft (RPA), have exploded in popularity, availability, and capability in recent years.[2] As batteries, cameras, flight control computers, and other key UAS components have become miniaturized,[3] cheaper, and plentiful, UAS

capabilities have greatly increased. Adversaries can now pilot a 70-mile per hour (mph), highly maneuverable four-bladed helicopter known as a "quadcopter," without any formal training by using a simple smart phone application. This new technology gives potential adversaries an additional and substantial offensive capability against friendly targets, with very little cost or logistics requirements. Gone are the days that a simple barbed-wire fence and a roving security patrol using standard-issue pistols and rifles will sufficiently protect our vital USAF aircraft.

Modern small UASs are versatile and can offset many current USAF capabilities. They are free to offensively maneuver and damage the Air Force's advanced stealth fighters and bombers, aerial refueling tankers, and cargo aircraft. Small UASs can also hold critical support facilities at risk. This "wicked" UAS problem will only get worse. We seek to build on the challenges presented in the *ASPJ* spring article on "Air Mines,"[4] and argue these new UAS capabilities allow their users to potentially negate advanced nation-state funded aerial and ground-based offensive and defensive systems, and the USAF needs a better capability to defeat these new small UASs.

We explore this topic by first defining and framing the issue of UAS proliferation. We then discuss possible adversary uses of UASs and detail counter-UAS (C-UAS) capabilities, assessing UAS strengths and weaknesses and showing ways adversaries could negate C-UAS defensive systems. We then recommend possible solutions and propose further research to counter ever-improving UAS capabilities.

The Problem of UAS Proliferation

As the information age continued, potential adversaries noticed the US military's UAS successes and developed their systems using commercially available off-the-shelf components. The USAF and DOD no longer had a monopoly on UAS supremacy. Enormous state-run UAS programs were no longer necessary to accomplish tactical and strategic goals. In August 2014, the terrorist group the Islamic State of Iraq and Syria (ISIS) posted Syrian military target videos that were taken with a simple, widely-sold DJI Phantom quadcopter.[5] More recently, ISIS has used drones as attack vehicles while using additional drones to film the results of these drone attacks.[6]

UASs are proliferating. The Federal Aviation Administration (FAA) estimated that approximately 1.9 million UASs were sold in the United States during 2016 and projects domestic sales of up to 4.3 million UASs annually by 2020.[7] This proliferation is global, with similar sales growth in China.[8] With as little as $130 in hand, virtually anyone can purchase a functioning UAS without any background check to discern hostile intentions.

Potential Adversary Uses of UASs

The low-cost, global proliferation and capabilities of UASs weighing less than 20 pounds make them worthy of specific focus.[9] Future adversaries could use these small systems to play havoc with military operations both in the air and on the ground, necessitating new actions to defend military assets and bases.

As indicated in the table below, several small UASs have payload capacity, extended range, and the ability to be global positioning system- (GPS) or pilot-guided

to locations with great precision. For example, the DJI Phantom 3 can fly for 23 minutes at speeds up to 37 mph, carrying a 2-pound payload, on one battery charge to a range of 13 miles if autonomously guided, and only costs $599–799.[10] While there are safeguards to protect airspace from inadvertent penetration by the Phantom 3, these safeguards are easily bypassed. The limitation restricting its maximum altitude to 120 meters (393 feet) higher than the takeoff location can be overridden to fly to its maximum altitude of 6,000 meters (19,685 feet) above sea level. Similarly, while the Phantom 3 has "geo-fencing" that uses its GPS position to determine if it is about to enter sensitive airspace, disabling the GPS antenna allows the pilot to visually navigate the quadcopter to any destination.[11]

Table. Sample of currently available commercial UASs[12]

Drone Name	Parrot "Airborne Night Swat	Parrot "Bebop 2"	SenseFly "Albris" (formerly eXom)	DJI "Phantom3 Advanced"	DJI "S1000"
Type of Aircraft	Palm-sized Quadcopter	Quadcopter	V-shaped Quadcopter	Quadcopter	Octocopter
Possible Hostile Mission	Surveillance, mortar spotting	Surveillance, "Kamikaze" attack	High resolution surveillance, "Kamikaze" attack	Surveillance, sabotage, explosive attack, "Kamikaze attack	Surveillance, sabotage, large-scale explosive attack, "Kamikaze" attack
Wingspan Size	7 x 7 inches	15 x 15 inches	22 x 32 inches	23 inches (diagonal)	41 inches (diagonal)
Empty Weight	63 grams / 2.1 ounces	500 grams / 1.1 pounds	1.8 kilograms / 4 pounds max takeoff weight	1.2 kilograms / 2.3 pounds	4.4 kilograms / 6.2 to 11 kilograms max takeoff weight
Payload: Includes Camera and Other Items	N/A – integrated camera	N/A – integrated camera	N/A – integrated camera	2 pounds	6.6 kilograms / 14.9 pounds
Flight Time	9 minutes	25 minutes	22 minutes	23 minutes	15 minutes
Speed	11 mph	37 mph	27 mph	37 mph	37 mph
Maximum Altitude	N/A	492 feet (150 meters)	N/A	19,685 feet (6000 meters)	Not specified by manufacturer
Pilot to UAS Maximum Range	20 meters / 65 feet	2 KM if used with Parrot Skycontroller	800 meters / 0.5 miles	5 kilometers / 3.1 miles when flying remotely	Not specified by manufacturer
Navigation system	Remote Control	GPS; Remote Control	GPS; Remote Control	GPS or GLONASS and Remote Control	GPS, remote Control
Cost	$129.99	$549.99 MSRP; $483.97 at Walmart	N/A – requires quote from manufacturer	$799.00 MSRP $598.00 at Walmart	$1,499 MSRP
Notes			1.2–mile video streaming range	2.7K streaming video	

This visual navigation is done via first-person video (FPV) capability. FPV allows the pilot to receive a real-time video image from a camera on the UAS, displayed in goggles worn by the pilot or onto an Android, iPhone or iPad type device. This provides a view to the pilot as if they were riding on the quadcopter which can enable the operator to execute evasive maneuvers or navigate clandestine routes while flying to a target.

While the DJI Phantom 3 can carry a single explosive, DJI sells higher-performance, heavy payload, eight-bladed octocopters that may be a bigger threat. The DJI S1000+ eight-bladed octocopter, designed for commercial cinematography, has a 15-minute flight endurance with a payload of 14.9 pounds and costs $1,499.[13] This payload equates to being able to haul six explosives or Thermite grenades while carrying a camera for FPV.

Thermite grenades only weigh 2 pounds and burn at 4,000 degrees Fahrenheit which is sufficient to melt through aircraft skin, rupture a fuel tank, and initiate an aircraft fire.[14] Aircraft-grade aluminum alloys melt at only 1,180-degrees Fahrenheit, and a ruptured fuel tank could sustain a fire by using the aircraft's own fuel.[15] Such an attack would damage or destroy an aircraft, yielding the adversary a psychological victory.

Additional potential uses for these UASs include emplacing spike strips on a runway to deflate aircraft tires, delivering debris to damage jet engines, dropping explosives on other targets, or even being used in a Kamikaze role.[16] Through the FPV, a UAS pilot could fly the UAS into an aircraft's engines during ground operations, on takeoff or landing, or even at extended ranges from the airfield. Attacking during the critical takeoff or landing phases of flight, the UAS could increase the chances of more damages or a catastrophic crash.[17] As the DJI Phantom 3 can climb to above 19,000 feet, attacks at significant distance from airports could complicate postaccident forensics as debris from that altitude scatters widely. The possibility of attacks at distance from an airfield increases the need for high-fidelity C-UAS detection capability at range.[18]

With several hundred dollars and the time to download an eBook and watch a YouTube video, anyone with a little technical expertise can build their own quad/hex/octocopter. These homebuilt UASs might be more capable than and circumvent the built-in restrictions of a commercially available UAS.[19]

Possible Solutions

Traditional base security measures are not designed to detect and defeat hostile UASs. Visual observers shooting small arms are ineffective due to the high speed, maneuverability, and survivability of a small UAS.[20] Traditional base/post security fences are also of limited value, as a pilot using FPV can fly over the barrier and then descend onto the target.[21]

This section will cover a series of systems in development that may help protect AF assets. These potential solutions range from man-portable systems to directed energy weapons, to broader systems of systems.

Drone Defender

The "Drone Defender" is a man-portable 20-pound system that looks a bit like a large fat rifle and is used to disrupt the command link between a UAS and the pilot. Its effective range, from friendly defender to the hostile UAS, is 400 meters. Future development will allow it to jam or spoof the GPS signal to prevent the UAS from using a signal for precise navigation.[22] Overall, the Drone Defender is dependent on a human observer detecting the UAS and then aiming and employing the device. If optimally employed, this system forces a lost-link flight path if it jams the correct command link frequency. Should the UAS escape the 30-degree beam width of the Drone Defender, the UAS may be able to resume normal operations.

An advantage of the Drone Defender is the nonpermanent effect can be stopped immediately if jamming creates an erratic or hazardous UAS flight path. Its disadvantage is the short 400-meter range, which would necessitate at least 25 devices and security personnel to effectively cover an entire airfield and the aircraft parking areas.[23] This makes Drone Defender a simple but resource-intensive, stop-gap measure until more capable C-UAS systems can be fielded.

Enhanced Area Protection and Survivability System

The US Army has tested the Enhanced Area Protection and Survivability System (EAPS) system that can engage a UAS up to 1 kilometer away by firing a 50 mm munition.[24] The system sends the inflight munition flight path corrections as the UAS maneuvers and then commands the munition to explode at the optimum range to shoot down the UAS.[25] This has collateral damage and fratricide concerns requiring careful system placement considerations and very strict rules of engagement.

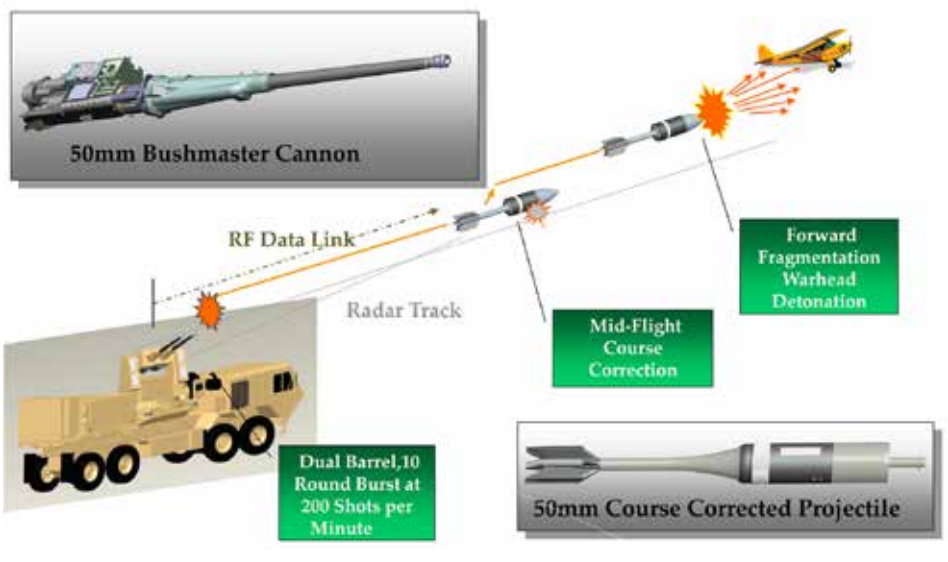

Figure 1. Enhanced Area Protection and Survivability System[26]

Counterrocket and Mortar System

The Northrup Grumman counterrocket and mortar) C-RAM) system is a current air-base defensive system deployed overseas that employs a radar-aimed Gatling gun to fire bullets at a rate of 2,000 rounds per minute to knock down rockets and mortars.[27] This system can also be employed against UAS threats to a range of 1.2 km. The kinetic collateral damage concerns require careful emplacement and employment procedures.

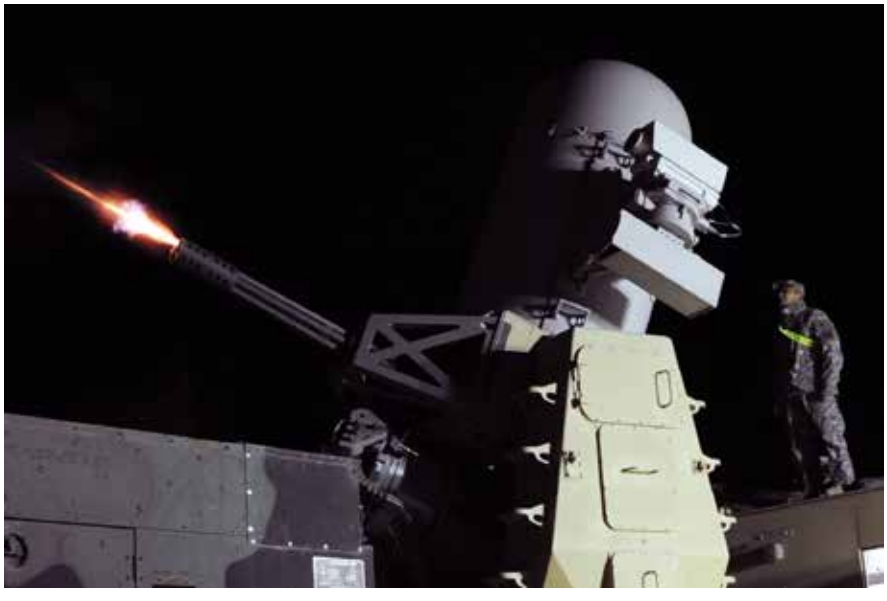

Figure 2. Army C-RAM System[28]

Compact Laser Weapon System "Silent Strike"

Boeing's Compact Laser Weapon System (CLWS) uses a destructive laser, cued by radar, and/or an electro-optical (EO)/infrared (IR) camera to track a hostile UAS.[29] The 10-kilowatt-class laser can heat and destroy UASs at ranges out to 2.5 km.[30] This system does not rely on knowing any UAS command frequencies or navigation techniques and is effective against any UAS modified to use self-contained guidance techniques. The system drawback is the potential for collateral damage short and long of the intended target which limits the engagement window. Laser energy also requires relatively clear air, unobscured by weather, smoke, or dust, etc. Carefully designing the air base defense layout would allow this system to be used to its maximum potential.

Counter-UAS Mobile Integrated Capability

The US Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC) has developed the Counter-UAS Mobile Integrated Capability

(CMIC). CMIC is a fully-developed, Soldier-tested, US government-owned, integrated and upgradeable counter-UAS system that can detect, identify, and then defeat a hostile UAS and its pilot.

Figure 3. Army CMIC System[31]

The CMIC system uses many common military parts to integrate multiple sensors into one easy-to-interpret display to provide the war fighter exceptional awareness of hostile UASs and the location of the pilot. The system can cue multiple EO, thermal, and electronic sensors to provide the operator high-fidelity threat information, to then coordinate nonkinetic or kinetic effects to bring the UAS down. CMIC also triangulates the source of the command signal to locate the pilot, which can enable launching a friendly UAS or ground forces to hunt the pilot.

To reduce logistical complexity, the design mounts the counter-UAS equipment onto current military vehicles and uses command and control devices that are widely available in the DOD. The CMIC also has a "flyaway kit" that eliminates the use of vehicles.[32] The CMIC utilizes a civilian SRC Inc. brand LSTAR Doppler radar to detect small UASs and even birds.[33] The bird detection capability gives it added utility for aiding manned aircraft in bird avoidance during the takeoff and landing phases of flight.

Drone Shield

Another spectrum for UAS detection is the unique acoustic signature of the electric motors and the spinning propeller blades. The Drone Shield Company makes acoustic sensors to detect UASs by their distinct noises and then references a library of acoustic signatures to determine the make and model. Drone Shield published the UAS detection range to be 1 km when using the Long-Range Sensor model, versus the shorter 100-meter range of the omnidirectional model.[34] UASs dropping weapons

from an altitude higher than the detection limit would potentially negate the acoustic detection system. Using the acoustic system as another sensor to correctly identify the UAS type will enable other defensive systems to properly jam or engage the threat.

High-Power Microwave Weapons

If US forces are deployed to a location with few electronic systems off-base, the use of high-power microwave (HPM) weapon systems might be feasible without collateral damage concerns. HPM weapons disrupt the electrical flow across unshielded wiring and circuit boards in electronic systems. An HPM weapon could be effective against UAS flight control computers to inflict a wide range of effects from barely disrupting a command signal to "frying" the circuit board to cause an immediate inflight failure of the UAS.[35]

Future scientific research should focus on developing high-power *pulsed* microwave weapons to defeat a UAS. The goal would be to create a pulsed-microwave effect to cripple hostile UASs without creating significant collateral energy which could damage friendly military and civilian systems.[36]

Airfield Modifications

Areas with tall buildings, trees, and so forth, that prevent direct line-of-sight to detect a UAS could benefit from tall fencing to channel the threat UASs into more observable areas. Canalizing attacking UAVs would allow security forces to focus the acoustic, radar and camera system capabilities into a more concentrated area. However, regardless of the counter-UAS system employed, fencing should be installed around and above all high-value assets that cannot suffer any UAS interference.

To aid in apprehending hostile or ignorant UAS pilots, a "Hunter Killer" UAS needs to be developed that can quickly fly toward a hostile UAS and use nonkinetic (possibly miniaturized *pulsed* HPM) or kinetic effects to disable the hostile UAS. This friendly UAS could also search for and identify the hostile pilot to allow forces to arrest the pilot (in the United States) or kinetically engage them (combat zone).

Potential Adversary Countermeasures

As many historical examples of military weaponry development have shown, as defensive measures to a new threat were discovered, the hostile actors made slight adjustments to their equipment to degrade the effectiveness of the new defenses. Although the previously detailed C-UAS systems are very capable, many of them rely on jamming the command link between the UAS and the pilot to force the UAS to execute a lost-link flight path. The programmed lost-link flight path might be to return to the home base, hover, or simply land immediately.[37] A hostile actor can bypass this lost-link problem by using the UAS autonomous flight mode which might utilize GPS, Galileo, GPS Aided GEO Augmented Navigation (GAGAN)/Indian Regional Navigation Satellite System (IRNSS), Bei Dou, or the Globalnaya Navigazionnaya Sputnikovaya Sistema (GLONASS) navigation constellations to control the flight path.[38]

If the GPS signal is jammed or spoofed; or if the UAS is purposely not GPS equipped to negate any jamming, spoofing or geo-fencing restrictions; an inertial navigation system (INS) could be used to guide the UAS.[39] An INS works by knowing the takeoff location and then sensing movement and drift to determine the UAS's current location as it flies to the target. An INS would eliminate any requirement for outside signals to navigate the UAS.

Another technique to negate communications link-jamming is for the hostile pilot to input the *target* coordinates as the "home base" so that when the jamming system breaks the command link with the pilot, the UAS actually flies *to* the target. Accurate target coordinates loaded into a UAS using the autonomous flight mode, without using the FPV feature, would only slightly degrade navigational accuracy. With just a little ingenuity and equipment modification, an adversary might be able to negate many of the current defeat mechanisms of C-UAS systems.

Current US laws also prevent utilizing the full capabilities of C-UAS defensive systems. The FAA considers a UAS a civil aircraft that must comply with safety requirements and regulations.[40] Because a UAS is considered a civil aircraft, security forces are prohibited from shooting down a UAS unless it is determined to be in the interest of national defense or for self-defense reasons.[41] Because it is virtually impossible to quickly determine the intent of a UAS, this current guidance could cause delays in responses which might give an adversary vital time to carry out their mission. The USAF must develop procedures and gain FAA and all necessary legal approvals to employ C-UAS defensive systems against any unknown UAS that is in the military airspace, whether it is over military land or not.

During the process of selecting overseas basing locations, the amount of clear areas around the airbase perimeter must be a big consideration to ensure the base is defendable. An extra-large buffer zone would allow for more aggressive C-UAS systems such as the C-RAM Gatling gun system or the use of a destructive laser system, such as the CLWS.

Recommendations

In the near term, the US government must determine who will lead solving the UAS problem. While the DOD can take the lead role in combat zones, within the United States, there are multiple civilian and military agencies working UAS issues, which can lead to confusion.[42] A whole of government approach is needed to make progress. The USAF, DOD, FAA, Department of Commerce, and the Department of Homeland Security (DHS) must quickly form an intergovernmental team to develop a whole of government approach to field effective counter-UAS defensive systems.[43] These agencies also need to solidify airspace defense procedures and make recommendations to Congress regarding more permissive legal authorities to preserve the USAF's ability to maintain air superiority.

The FAA and DOD must immediately initiate a more aggressive countrywide UAS education campaign. "No Drone Zone" signage placed around military airfields and near the approach and departure corridors with phone numbers to call to report illegal UAS activity would improve education and enforcement efforts.[44] Military

public affairs engagements with the local media would minimize the number of UAS pilots unaware of the new rules. A well-educated public should reduce the number of innocent airspace incursions thereby allowing security forces to quickly decide hostile intent and immediately take appropriate action.

If laws cannot be adjusted to authorize shooting down a hostile UAS, then another option is to increase the punishment for airspace and procedural violations.[45] Class D (airspace with an operating air traffic control tower such as most military air bases) and restricted airspace (typically military bombing ranges) violations pose the greatest hazard since these are generally congested with very fast military aircraft.[46] The general public will not take the new UAS flight rules seriously unless the punishments for being an ignorant or brazen UAS pilot are widely known and consistently applied.[47]

USAF security forces and other DOD security units, in close coordination with the lead law enforcement agencies, must conduct regular training exercises that include hostile UAS scenarios. The reaction to a hostile UAS flying into military airspace while transiting multiple police jurisdictions must be well-rehearsed, legally reviewed, and trained to the same level as a "front gate-runner" scenario. For example, if someone drives their car from off base through an air base checkpoint without stopping, the guards are trained how to warn the driver, then take prudent and proportional actions up to, and including, deadly force. Security forces must have a similarly well-rehearsed response to a UAS violating military airspace, so they are not paralyzed by indecision, or overreact with pistols and rifles and cause catastrophic damage to an aircraft in the background.

Until adequate C-UAS defensive systems are procured and can be fully employed, a system-of-systems approach is likely required to detect a UAS across the various energy spectrums to cue sensors and weapons to defeat the UAS before it can complete its nefarious mission. Improving airfield and ramp lighting, or adding additional low light EO and thermal camera systems, are relatively low-cost and familiar solutions.[48] Good coordination with a cooperative civilian population will enable emplacement of sensors onto existing infrastructure to provide surveillance of airfield approach and departure corridors. These low-cost surveillance systems at least enable security forces to be slightly more aware of someone flying a hostile UAS near their airfield.

To minimize fratricide to friendly electronic systems, applicable research labs must test the interoperability of C-UAS systems with existing airfield and DOD systems. Additional testing is needed to learn the effects of integrating directed energy weapons, the UAS detection radars, and other sensors to ensure safe interoperability with aircraft navigation and communication systems, flight control computers, instrument landing systems, GPS reception, and air traffic control (ATC) radars. These systems and their human operators all need evaluation to ensure C-UAS systems will not cause hazards for military operations.

Procedures must be perfected between the C-UAS operators and the ATC agencies to quickly communicate the location of hostile UASs to direct evasive maneuvers to airborne aircraft. Close coordination is also required when firing weapons to prevent fratricide. It is beneficial that most C-UAS weapon systems have a short em-

ployment time, in the realm of several to tens of seconds, which should minimize disruption to flight operations.[49]

Because of its relative maturity and ability to continuously and automatically fuse multiple sensors into a complete battlefield picture, at the time of this writing, the CMIC is the most promising system available. The approximate cost for the CMIC system, without vehicles, is $1 million for the system and $1.1 million for the LSTARS radar.[50] Because of line-of-sight issues near an airfield caused by topography, buildings, trees, and so forth, multiple radars or installing the sensors on a tall tower may be required to have 360-degree visibility. CMIC's advantages are its multiple sensor fusion combined with multiple engagement methods. As technology improves, other systems are likely to overtake CMIC in capability, but our research strongly suggests the optimum system in the future will involve fusing disparate sensors to detect even the smallest of UASs and provide a variety of defense mechanisms able to engage threats ranging from single UASs to UAS swarms.

As UAS technology continues to improve in the next five to 10 years, civilian UASs will become more popular and useful to civilian industries, thereby increasing the overall number of friendly UASs flying at higher altitudes in congested airspace.[51] Because of this increased congestion, robust detection and flawless inflight identification is necessary to quickly target hostile or suspicious UASs.

Because of airspace saturation with UASs, manned aircraft will soon need onboard detection capabilities or be linked into the ground-based sense and avoid systems to evade single and swarmed UAS airborne threats.[52] The addition of thousands of UASs flying in the low-altitude structure, when combined with the usual bird hazards, could make military low-altitude flying training more hazardous. This risk could restrict low-level training to such confined areas that the training value will be nil, thereby limiting military aircraft combat maneuvering options. The development of onboard UAS avoidance equipment must start immediately.

Conclusion

The threats from hostile UASs will continue to get worse at an exponential rate because of improving capabilities and the sheer quantity being sold in the civilian marketplace. The risk of a major, catastrophic loss of life because of a collision between a hostile UAS and a manned aircraft continues to rise. The USAF must coordinate and accelerate all efforts to acquire a counter-UAS system that will protect aircrew and aircraft.

Although no single system will negate every conceivable UAS threat, the AMRDEC CMIC system, or a more advanced system like it, appears to be the best system today to solving the wicked problem of hostile UAS interference. The blending of multisensor fusion with multiple engagement options against hostile UASs is a powerful combination. While such systems may seem expensive, being proactive can save many lives and millions of dollars while also denying adversaries another attack method to further their goals. One irreplaceable $143 million F-22 "Raptor" or a $98 million F-35 "Lightning II" Joint Strike Fighter lost to a $799 hostile UAS will make a $2.1 million price tag for a C-UAS system, like the AMRDEC CMIC, look

very affordable.[53] The AMRDEC system also provides an additional advantage of detecting birds that pose a hazard to aviation operations while continuously standing guard to defeat a hostile UAS.

This article recommends purchasing the AMRDEC CMIC or similar system and maintaining and operating it with a small crew of USAF personnel as the best technical solution to defend an airfield 24 hours a day. At the same time, the legal authorities to employ all its capabilities must be obtained. The DOD, DHS, FAA, USAF, Department of Transportation, and the Department of Commerce are some of the key entities that must form an interdepartmental team. This team must collaborate and recommend legal authority changes to Congress to solve the UAS problem.

Security personnel must have the legal authorities to declare any unauthorized UAS flying in military airspace a hostile threat and take action whether the hostile UAS is over civilian or military property. Security forces must be allowed to immediately nonkinetically engage the threat within friendly territory, or kinetically engage the system if in a combat zone. If the hostile UAS is neutralized off military property, the USAF must have procedures for off-base civilian law enforcement assets to secure the downed UAS and apprehend the offending pilot.

If the fictitious airfield described in the introduction were properly equipped with C-UAS systems, the attack would have been an air superiority success story instead of a nightmare scenario. It is only a matter of time before our nation's adversaries will utilize these incredibly capable UAS threats to attempt to defeat the most advanced air force in the world. ✪

Notes

1. Richard Whittle, "Military Exercise Black Dart to Tackle Nightmare Drone Scenario," *New York Post*, 25 July 2015, http://nypost.com/2015/07/25/military-operation-black-dart-to-tackle-nightmare-drone-scenario/. The 2015 Black Dart exercise was designed to test counter drone systems against 55 drone systems encompassing a wide range of drone sizes and capabilities. The focus of the exercise was on smaller drones due to the recent events of small drones flying near prominent politicians. German chancellor Angela Merkel's incident in Dresden two years ago involved an unmanned aircraft system (UAS) flying near her, and the Japanese prime minister Shinzō Abe had a drone land on top of his residence. This article stated that British officials are concerned the Islamic State Iraq and Syria (ISIS) will try to bomb festival crowds using small drones.

2. Since a significant amount of unmanned aerial system literature comes from the Federal Aviation Administration (FAA), the term *unmanned aerial system* (UAS) will be used in this article and is synonymous with drone, remotely piloted aircraft (RPA) or unmanned aerial vehicle (UAV).

3. Leslie Hauck and John Geis, "Air Mines: Countering the Drone Threat to Aircraft," *Air and Space Power Journal* 31, no. 1, Spring 2017, 26–40.

4. Ibid. These two articles emanate from Air University's newly-created Airpower Research Task Force and associated Airpower Vistas elective program.

5. Jamie Conliffe, "ISIS Militants Use Same Drones as Ordinary Folks," *Gizmodo*, 29 August 2014, http://gizmodo.com/isis-militants-use-the-same-drones-as-ordinary-folks-1628376186. ISIS showed how a widely available UAS could easily be used for tactical purposes.

6. Jody Warrick, "Use of 'Weaponized' Drones by Islamic State Spurs Terrorism Fears," *Chicago Tribune*, 27 February 2017, http://www.chicagotribune.com/news/nationworld/ct-islamic-state-drones-20170225-story.html.

7. "FAA Releases 2016 to 2036 Aerospace Forecast," https://www.faa.gov/news/updates/?newsId=85227, 24 March 2016.

8. Paul Bedard, "Drone Sales Surge 167% to 4.3 million, U.S. leads but China Catching Up," *Washington Examiner*, 29 May 2015, http://www.washingtonexaminer.com/drone-sales-surge-167-to-4.3-million-u.s.-leads-but-china-catching-up/article/2565240. This article states that 4.3 million consumer drones, worth 1.7 billion dollars, were sold worldwide in the first five months of 2015, which was a 167 percent jump in only two years.

9. Another very capable quadcopter is made by Mobile Recon Systems. Their Kitty Hawk HDX4 Supreme Heavy Lift Quadcopter has a payload of 22 pounds (total weight of up to 41 pounds) and a 30-minute flight time. See http://www.mobilereconsystems.com/?page_id=32 for more details.

10. DJI website accessed 2 February 2016, http://store.dji.com/compare-phantom-3. Prices have dropped by $200 in two months, making UASs even more affordable. Autonomous flight-range limit would be approximately 13 statute miles (35 mph x 23 minutes = 13.41 statute miles), assuming no wind conditions; and DJI website accessed 6 December 2015. Payload weight also includes the camera which is necessary for the first-person video capability, but would not be needed for autonomous flight, http://wiki.dji.com/en/index.php/Phantom_3_Advanced#GENERAL_FEATURES.

11. Geo-fencing is only accurate if the UAS has been updated with the most recent information. If an airport's airspace changes, but the UAS is operating with old data, the geo-fencing feature will be ineffective at preventing an airspace violation.

12. Data in the table comes from: https://www.parrot.com/us/minidrones/parrot-airborne-night-swat#parrot-airborne-night-swat-details for the Parrot Airborne Night Swat; https://www.parrot.com/us/Drones/Parrot-bebop-2 for the Bebop-2; http://drones.specout.com/l/1103/senseFly-albris for the10-V-Palmer-Geis.indd 113 4/27/2017 10:10:56 AM114 | Air & Space Power JournalAlbris; http://www.dji.com/phantom-3-adv/info#specs for the DJI Phantom III; https://www.dji.com/spreading-wings-s1000 for the DJI S1000.

13. DJI company website, accessed 27 February 2017, http://www.dji.com/product/spreading-wings-s1000-plus. This price includes the global positioning system (GPC) receiver and guidance unit as well as some special flight controller logic to handle an engine failure, thereby making it even harder to shoot it down since it can handle an engine failure. See also *Spreading Wings S1000+ User Manual V 1.4*, available at http://www.dji.com/spreading-wings-s1000-plus/info#downloads.

14. Federation of American Scientists (FAS) Military Analysis Network, accessed 6 December 2015, AN-M14 TH3 incendiary hand grenade, http://fas.org/man/dod-101/sys/land/m14-th3.htm. This site references US Army Field Manual (FM) FM23-30 *Grenades and Pyrotechnic Signals*, 27 December 1988.

15. Aviation Metals Inc., company website, accessed 8 December 2015, http://aviationmetals.net/aluminum_sheet.php. Standard aircraft-grade aluminum alloys melt at 1,180-degrees Fahrenheit/580-degrees centigrade. These aluminum alloys are commonly used for aircraft structures and aircraft skins to form wings, external fuel tanks, or the fuselage.

16. Aardvark company website accessed 9 December 2015, https://www.aardvarktactical.com/products/caltrops. Tire deflation Caltrops spikes would be very effective. These spikes have three points and always land with a point up. Multiple spikes can be strung together to any length to meet UAS payload weight limits. Once the aircraft tire is punctured, the spike will stay in the tire to allow rapid deflation. Although aircraft tires are rugged, the high pounds per square inch makes them vulnerable to violent deflation if pierced.

17. Aviation Safety Boeing Commercial Airplanes, *Statistical Summary of Commercial Jet Airplane Accidents, Worldwide Operations, 1959–2014,* August 2015, 20, *http:*//www.boeing.com/resources/boeingdotcom/company/about_bca/pdf/statsum.pdf. These data show from 2005–2014 that 13 percent of fatal accidents occurred during takeoff and initial climb phases, and 48 percent of fatal accidents occurred during final approach and landing phases. See also Hauck and Geis, "Air Mines," 26–40.

18. Rollin Bishop, "Record-Breaking Drone Swarm Sees 50 UAVs Controlled by a Single Person," *Popular Mechanics*, 16 September 2015, http://www.popularmechanics.com/flight/drones/news/a17371/record-breaking-drone-swarm/. This demonstration was conducted by the Naval Postgraduate School and proved the ability to control 50 UAVs with just one pilot. The UAVs could maintain safe separation and adhere to the commands of the one pilot; and Steve Crowe, "Tests Show Drone Strikes Could Cause Jet Engine Failure," *Robotics Trends*, 28 October 2015, http://www.roboticstrends.com/article/tests_show_drone_strikes_could_cause_jet_engine_failure. "Researchers at Virginia Tech's College of Engineering

say drones as small as 8 pounds will have devastating effects if sucked into the turbofan engines of commercial aircrafts." Currently the FAA rules don't require aircraft engine manufacturers to test against the damaging effects of ingesting a UAS (just birds). Hard plastic/metal parts and the lithium-ion batteries can cause massive damage to jet engines.

19. Small Drone Reviews *Best eBook Drone Tutorial—Build Your Own Quadcopter,* http://smalldronesreview.com/2015/10/10/how-to-build-your-own-quadcopter-drone-best-bookebook-tutorial/. This website has many eBooks to cover a range of homebuilt quadcopter designs.

20. Kelsey D. Atherton, "How Hard Is It to Shoot Down a Small Drone?," *Popular Science*, 14 April 2014, http://www.popsci.com/article/technology/how-hard-it-shoot-down-small-drone-video-0. Big Sandy Shoot is a group of machine gun enthusiasts in Arizona who flew small UASs in front of their firing line. The machine gunners required hundreds of rounds and many passes of the UAS flying directly in front of the firing line to have even a minute for the chance of hitting the cooperatively flown UAS. Their assessment was that it was very difficult to hit the small UAS. The small UASs sustained bullet strikes to noncritical sections of the airframe and were still able to fly.

21. Michael S. Schmidt, "Airmail via Drones is Vexing for Prisons," *New York Times*, 22 April 2015, A13, http://www.nytimes.com/2015/04/23/us/drones-smuggle-contraband-over-prison-walls.html?_r=0. Prisons are starting to experience an increase in UAS use to deliver contraband (drugs, weapons, cellphones, etc.) to prisoners. The UASs are flown over the high barbed-wire fences and are either landing, or simply dropping the objects onto prison property. If a UAS can successfully bypass armed guards, cameras, and fencing at a relatively small exercise yard at a medium or maximum security prison, it should be incredibly easy to fly over a USAF airfield perimeter fence that spans for many miles. Even if fencing was installed over a prison exercise yard to prevent a UAS from landing, the mesh would have to be small enough to prevent smugglers from dropping small items through the mesh.

22. Kelsey D. Atherton, "This Device Turns Any Gun into an Anti-Drone Ray," *Popular Science,* 15 October 2015, http://www.popsci.com/dronedefender-is-an-anti-drone-rifle-attachment.

23. Using a calculation that assumes security personnel with Drone Defenders would be no more than 800-meters apart (400-meter range for each Drone Defender), a standard 11,000-foot long runway would require at least 10 spotters/Drone Defenders to cover the length/sides of the runway, plus five more to cover a small parking ramp, plus at least 10 more spotter/Drone Defenders to cover two miles of the approach and departure corridors. In total, at least 25 security personnel would be assigned to spotter/Drone Defender duty 24/7. More personnel might be required to utilize night vision devices during hours of darkness. Also, these personnel would be outside (not in an enclosed vehicle or watchtower) to have any reasonable chance of hearing the incoming UASs.

24. David Szondy, "US Army Tests Drone-killing 50 mm Cannon," *Gizmag*, 11 October 2015, http://www.gizmag.com/us-army-eads-anti-drone-system/39781/.

25. Edward Lopez, "Army Engineers Demonstrate Anti-drone Technology" *Army.mil*, 5 October 2015, http://www.army.mil/article/156634/Army_engineers_demonstrate_anti_drone_technology/.

26. Ibid.

27. Andrew Tarantola, "The C-RAM Centurion Tears up Warheads with a Stream of Hot Lead," *Gizmodo*, 4 April 2012, http://gizmodo.com/5907237/the-c-ram-centurion-tears-up-warheads-with-a-stream-of-hot-lead.

28. Photo courtesy of Senior Airman Brittany Bateman, through Wikipedia Commons, https://commons.wikimedia.org/wiki/File:C-RAM_test_fire_JBB_Iraq.jpg.

29. Electro-optical (EO) cameras are similar to standard television cameras, relying on light to capture an image, whereas the infrared (IR) camera uses a thermal difference between the UAS and the background to generate an image. Small UASs typically have a very small thermal signature due to the electric motors (versus gas-powered) that power the propellers.

30. Boeing company website accessed 10 December 2015, http://www.boeing.com/features/2015/08/bds-compact-laser-08-15.page. This destructive laser shows great promise for use in more congested areas since it isn't as powerful as some other destructive lasers which were designed for use on the open seas.

31. E-mail between Mr. Steve Bramlett, Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC) program manager and the author.

32. Briefing slide from Bramlett on 26 January 2016 (Annex C). The AMRDEC "flyaway" kit is all the electronics but isn't mounted onto a vehicle. For austere overseas air bases, this fly-away kit would

drastically reduce the logistics footprint. Eliminating a vehicle would save thousands of dollars by not maintaining a vehicle that is simply a mount for the Counter-UAS Mobile Integrated Capability (CMIC) equipment.

33. Syracuse Research Corporation (SRC) Inc., company website accessed 10 December 2015, http://www.srcinc.com/what-we-do/radar-and-sensors/lstar-air-surveillance-radar.html. This radar system has several versions for different applications.

34. Drone Shield company website, accessed 2 February 2016. The acoustic sensors are a lower cost solution or an addition to a complete system. These acoustic sensors can differentiate from aircraft and UAS noise signatures. The exact range of detection for the omnidirectional sensor is not published on the company website. However, the long-range sensor is published to detect UASs up to 1 kilometer and states it is 10 times farther than the standard omnidirectional sensor which would imply only a 100-meter range for the omnidirectional sensor. The Drone Shield system can provide alerts to security personnel when a UAS is detected. Information about the omnidirectional sensor can be found at https://www.droneshield.com/omnidirectional-sensor. Information about the long-range sensor can be found at https://www.droneshield.com/long-range-sensor.

35. If high-power microwave (HPM) weapons can't be miniaturized or tailored to reduce collateral damage, the use of stronger weapons could be used at austere locations since there wouldn't be the collateral damage concerns compared to modern urban areas. There would still be concerns about affecting coalition aircraft and electronic systems, but that risk could be mitigated through smart HPM weapon layout on the airfield as well as good coordination when employing HPMs to ensure no manned aircraft are harmed. If electronic systems are hardened/shielded against HPM, the HPM weapon will be ineffective.

36. Boeing Company website, "CHAMP—Lights Out," 22 October 2012, http://www.boeing.com/features/2012/10/bds-champ-10-22-12.page. The Boeing Counter-electronics HPM advanced missile project (CHAMP) weapon is a great example of a small size HPM weapon and the selective effects that are possible. It can fire the selective high-frequency radio wave energy at specific buildings and targets.

37. Da-Jiang Innovation (DJI) website accessed 6 December 2015, http://www.dji.com/product/phantom-3-standard/feature?www=v1. There are several other lost-link options with different UAS brands. Also, some minor flight control malfunctions and GPS and controller signal interruptions will cause "fly-aways" where the UAS is unresponsive to controller inputs and fails to follow the preprogrammed lost-link profile. Fly-aways could be an innocent source of airspace incursions.

38. US GPS is the commonly used global positioning system. Galileo is a European GPS constellation with a 1-meter accuracy. Bei Dou is the Chinese GPS navigation system. GPS-aided, GEO-augmented Navigation (GAGAN) is a partially land-based component of the Indian navigation system which augments the US GPS constellation. In addition to GAGAN, India is creating its GPS-like navigation system with seven satellites currently part of its Indian Regional Navigation Satellite System (IRNSS). Global-naya Navigazionnaya Sputnikovaya Sistema (GLONASS) is the Russian navigation system.

39. SBG company website accessed 20 January 2016, http://www.sbg-systems.com/products/ellipse-n-miniature-ins-gps. The Ellipse-N miniature Inertial Navigation System (INS) also incorporates GPS+GLONASS/Bei Dou information to keep the INS very accurate and ready to provide navigation info if the GPS signal is jammed. This system is very lightweight and small enough to be installed onto a quadcopter/UAS. This system eliminates the need for any outside signals to navigate a UAS to the target.

40. Federal Aviation Administration (FAA) guidance, "Law Enforcement Guidance for Suspected Unauthorized UAS Operations," accessed FAA website 27 January 2016, http://www.faa.gov/uas/law_enforcement/. An applicable section from this guidance: "A UAS is an 'aircraft' as defined in the FAA's authorizing statutes and is therefore subject to regulation by the FAA. 49 U.S.C. § 40102(a)(6) defines an aircraft as "any contrivance invented, used, or designed to navigate or fly in the air." The FAA's regulations (14 C.F.R. § 1.1) similarly define an aircraft as "a device that is used or intended to be used for flight in the air." Because an unmanned aircraft is a contrivance/device that is invented, used, and designed to fly in the air, it meets the definition of aircraft. The FAA has promulgated regulations that apply to the operation of all aircraft, whether manned or unmanned, and irrespective of the altitude at which the aircraft is operating. For example, 14 C.F.R. § 91.13 prohibits any person from operating an aircraft in a careless or reckless manner so as to endanger the life or property of another."

41. The right to self-defense comes from common law. Refer to the 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces (U)," See also: The Judge Advocate

General's Legal Center and School, "Domestic Law, 2013 Handbook for Judge Advocates" US Army Center for Law and Military Operations, 2013. This handbook is also available electronically at https://www.jagcnet.army.mil/.

42. Ben Wolfgang, "FAA's Failure to Regulate U.S. Drone Boom Creates Climate of Confusion," *Washington Times*, 6 January 2015, http://www.washingtontimes.com/news/2015/jan/6/faa-failure-to-regulate-us-drone-boom-creates-clim/?page=all.

43. According to the Department of Homeland Security (DHS) website, their No. 1 core mission is to: "Prevent terrorism and enhancing security." DHS states that "Protecting the American people from terrorist threats is our founding principle and our highest priority." The Department of Homeland Security's counterterrorism responsibilities focus on three goals: (1) prevent terrorist attacks; (2) prevent the unauthorized acquisition, importation, movement, or use of chemical, biological, radiological, and nuclear materials and capabilities within the United States; and (3) reduce the vulnerability of critical infrastructure and key resources, essential leadership, and major events to terrorist attacks and other hazards. DHS website accessed 2 February 2016, http://www.dhs.gov/prevent-terrorism-and-enhance-security.

44. The "No Drone Zone" info can be found at the FAA website, https://www.faa.gov/uas/no_drone_zone/.

45. Law Enforcement Guidance for Suspected Unauthorized UAS Operations, Version 3, Issued 11 August 2016, pp. 5, 8 www.faa.gov/uas/resources/law_enforcement/media/faa_uas-po_lea_gu... Accessed 29 March 2017, regarding enforcing UAS violations:

> It is extremely difficult to provide a "one size fits all" guide to cooperative investigation of suspected unauthorized UAS operations...The FAA may assess civil penalties up to $27,500. Criminal penalties include fines of up to $250,000 and/or imprisonment for up to three years."

46. Federal Aviation Administration educational briefing, "Airspace, Special Use Airspace, and Temporary Flight Restrictions," 7, accessed 27 January 2016, https://www.faasafety.gov/files/gslac/courses/content/42/565/Airspace,%20Special%20Use%20Airspace%20and%20TFRs%20-%20Text%20Only.pdf.

47. UAS pilots are required to become registered UAS pilots by logging on to the FAA website https://www.faa.gov/uas/registration/ and paying five dollars. The UAS pilots then print off a registration number to affix to their UAS to allow authorities to know who owns the UAS if it is found.

48. The forward looking infrared (FLIR) systems website accessed 6 December 2015, http://www.flir.com/surveillance/display/?id=63907. FLIR technologies have developed incredible thermal camera capabilities such as their Ranger high-resolution camera (HRC).

49. Liz Klimas, "'Silent Strike' Laser Weapon Burns Down a Drone in 15 Seconds," *The Blaze*, 28 August 2015, http://www.theblaze.com/stories/2015/08/28/silent-strike-laser-weapon-burns-down-a-drone-in-15-seconds/. This article highlights the Boeing "Silent Strike" Compact Laser Weapon System and how it can damage a test UAS in only 15 seconds of firing its laser weapon.

50. Cost estimate is a rough order of magnitude from Steve Bramlett, the counter-UAS mobile integrated capability (CMIC) program lead at AMRDEC, via e-mail to the author on 9 December 2015.

51. Samuel Gibbs, "Nearly 300,000 Civilian Drones Were Registered in US in 30 days," *The Guardian*, 26 January 2016, http://www.theguardian.com/technology/2016/jan/26/300000-civilian-drones-registered-in-us-compulsory. UAS registration with the FAA was occurring approximately 10,000 times a day after the FAA formalized the requirement for UAS pilots to register. Although this implies registered pilots will attempt to comply with regulations, this number doesn't account for illegally made and illegally flown UASs.

52. Kelsey D. Atherton, "FAA Tests System to Let Drones Sense and Avoid Obstacles," *Popular Science*, 13 November 2015, http://www.popsci.com/faa-tests-drone-obstacle-avoidance-system. Sense and avoid systems can use cellular phone networks to relay the locations of UASs to aid the UASs in deconflicting their flightpaths. A noncooperative (hostile) UAS might be able to stay off of this system to allow more freedom to operate undetected.

53. Joint Base Eustis–Langley website accessed 29 March 2017. The 1st Fighter Wing flies the Air Dominance multirole F-22 fighter valued at $143 million each. See http://www.jble.af.mil/About-Us/Fact-Sheets/Display/Article/257723/f-22-raptor. According to the Lockheed Martin website on 6 December 2015, it states a USAF F-35 variant (F-35A) will cost $98 million, https://www.f35.com/about

/fast-facts/cost. The AMRDEC CMIC flyaway kit is estimated to be $2.1 million according to Steve Bramlett at AMRDEC via e-mail to the author on 9 December 2015.

Lt Col Thomas Palmer, USAF

Colonel Palmer is assigned to the Air War College, Air University, Maxwell AFB, Alabama. He is a US Air Force pilot, highly experienced in the F-15E Strike Eagle and its tactical employment and aircrew training processes. He also has extensive experience serving in South Korea, first as an air liaison officer with the US Army, and years later on a joint staff at the US Forces Korea headquarters in Seoul, South Korea. Colonel Palmer also recently commanded an F-15E formal training squadron at Seymour Johnson AFB, North Carolina.

Dr. John P. Geis II, Colonel, USAF, Retired

Dr. Geis (MA, Air University; MS, Auburn University; BA, MS, and PhD, University of Wisconsin) is the director, Airpower Research Task Force at Maxwell AFB, Alabama. He was the chief meteorologist of WISC-TV before entering active duty in 1983. His Air Force career spanned training and combat operations in which he flew the T-37, AT-38B, T-43, two variants of the F-111, and the AC-130H special operations gunship. A distinguished graduate and the Commandant's Award winner at Air Command and Staff College, Colonel Geis coauthored the Alternate Futures monograph for the Air Force 2025 Study. In 1998–2000, he served as the director for strategic planning, doctrine, and force integration for all US Air Force special forces. Beginning in 2001, Colonel Geis served as the director, US Air Force Center for Strategy and Technology, a position he held for eight years. During this time, he and his team created what is now known as the Blue Horizons Program, which examines the strategic implications of emerging technology.