Booz | Allen | Hamilton

TAKING AN ENTERPRISE INTEGRATION APPROACH TO COUNTER UNMANNED AIRCRAFT SYSTEMS

Brian Abbe
Senior Vice President
Abbe_Brian@bah.com

Troy Abbott
Distinguished Engineer
Abbott_Troy@bah.com

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER

TAKING AN ENTERPRISE INTEGRATION APPROACH TO COUNTER UNMANNED AIRCRAFT SYSTEMS

UNDERSTANDING THE COMPLEX, FAST-EVOLVING THREAT

Ever since the Austrian military deployed a flotilla of pilotless, bomb-laden balloons over a besieged Venice in 1849, planners have been endeavoring to exploit unmanned aircraft systems (UASs) for military pursuits. And while the U.S. military has led many of these advancements in recent decades, we have reached an inflection point today in which the rapid commercialization of UAS technologies has enabled any adversary – however small or poorly resourced – to harness these advanced capabilities.

Inexpensive, readily available, versatile, and difficult to detect and defeat, UASs have quickly emerged as mainstay assets in the arsenals of many adversaries and potential adversaries. They can strike enemies with bombs or grenades, perform reconnaissance and surveillance, and provide forward air control, including laser designation, for indirect or direct fires, among other tasks.

ISIS militants, for example, employed commercial-off-the-shelf quadcopters – available for about $2,000 and outfitted with weapons that fired 40-millimeter munitions – to torment U.S. and Iraqi forces during the Mosul offensive in 2016, said Gen. Raymond A. Thomas III, commander of U.S. Special Operations Command. “This last year’s most daunting problem,” he said, “was an adaptive enemy who, for a time, enjoyed tactical superiority in the airspace under our conventional air superiority in the form of commercially available drones and fuel-expedient weapons systems, and our only available response was small arms fire. There was a day when the Iraqi effort nearly came to a screeching halt, where literally over 24 hours there were 70 drones in the air. At one point, there were 12 ‘killer bees,’ if you will, right overhead and underneath our air superiority.”[1]

As the ISIS example demonstrates, the attributes of today’s commercially available UASs make them ideal platforms for irregular forces. “This is different from trying to tackle unmanned systems used by state actors – these are terrorists using a commercial product modified to drop a small bomb or self-destruct. It’s a serious threat to our ground troops,” said Sen. Joni Ernst, R-Iowa, chairman of the Senate Armed Services Subcommittee on Emerging Threats and Capabilities.[2]

In many respects, the UAS threat of today is similar to the improvised explosive device (IED) threat that plagued deployed U.S. forces in Afghanistan and Iraq a decade ago. Like IEDs, UASs are asymmetric threats typically employed against targets of opportunity and offering great potential to cause grave harm, sow fear, and disrupt military operations. The use cases are many and could include strike missions against navy ships, forces on maneuver, and forward operating bases; directed collisions with aircraft; recon and surveillance sorties; and target spotting for indirect fires.

And like IEDs, UASs come in a wide variety of variants and threat profiles. An IED can be deployed in many configurations and triggered by a timer, radio, mobile phone, wireless, command wire, long fuse, or victim-operated tripwire, infrared beam, or pressure pad. Likewise, UASs range from low-flying hobbyist versions to high-altitude, military-grade variants. Hobbyist UASs are easily purchased commercially and rely on proximate command and control, whereas military variants can carry advanced sensor packages and communications links that enable long-range command and control or can even be pre-programmed. They come in a variety of fixed-wing and rotary-wing configurations and payloads also vary widely, regardless of whether they are high- or low-end models, to include cameras, laser designators, radio frequency collection devices, various sensor packages and munitions.

Traditional force protection measures, such as short-range air defense (SHORAD) systems, often cannot detect, track and defeat UASs because of their relatively small size, composite materials, small radar and electromagnetic signatures, and quiet operation. Depending on the nature of the specific threat, detection may require optical or acoustic sensors, signals intelligence sensors, or radar, or a combination of those capabilities. Once detected, the task of neutralizing a UAS threat may require directed energy or kinetic intercepts, electronic jamming, or other approaches. As with IEDs, planners will need to design flexible approaches in the countermeasures they develop for UASs.

But notably *unlike* the IED threat, the UAS threat is rapidly evolving, proliferating, and growing more sophisticated due to an accelerating global marketplace. More than 30 countries, including Iran, China, Russia, and North Korea, have armed UASs or are developing the capability to build them, while at least 90 countries, as well as some non-state actors, possess unarmed UASs, according to the Center for a New American Security.[3] In addition to ISIS, numerous non-state actors possess and employ UASs for combat purposes. These include the Houthi rebels in Yemen, the Lebanese militant group Hezbollah, the Palestinian group Hamas, the Kurdish Peshmerga, the Revolutionary Armed Forces of Colombia (FARC), assorted terrorist and rebel groups in Syria, Libya, and Ukraine, as well as Colombian and Mexican drug cartels.[4] Further proliferation is inevitable as countries such as Israel, China, and Iran continue to sell UASs on the global market and other countries develop their own offerings.

As a result, most experts expect to see continued advances in UAS technology that will further complicate the challenge of countering UASs on the battlefield. For example, future UASs are expected to employ: encrypted communications links; increased ranges, payloads, and endurance; multi-vehicle cooperative control, allowing a single operator to control several vehicles in flight simultaneously; visual-aided navigation to allow precision Global Positioning System (GPS)-independent navigation, which would eliminate vulnerability to jamming and spoofing attacks; and "sense-and-avoid" systems that allow them to navigate autonomously around obstacles.

As reported recently in Joint Force Quarterly: "Although current state-of-the-art small unmanned aircraft system (sUAS) capabilities are sufficiently threatening, we are on the cusp of technological advances that will make the sUAS exponentially more deadly. The asymmetric nature of the sUAS, especially when considering swarm tactics, makes the technology difficult to defend against."[5]

Today's Counter UAS (C-UAS) Landscape

Unable to effectively counter today's emerging UAS threat, vendors and military program managers have launched a rush of activity to research, develop, and demonstrate potential solutions. Most of those efforts focus on "point solutions" that address specific threat scenarios and employ specific technologies and approaches tailored for those scenarios. Consequently, these efforts are insufficient to address the full spectrum of the C-UAS challenge.

Moreover, the lack of a unified joint strategy has left these efforts fragmented and disjointed – the surface ship community is approaching the threat and its solutions differently than the facilities community, the deployed land forces community, the aviation community, or the UAV community, for example.

Another concern is that most C-UAS efforts today lack an appreciation for the full complexity of the challenge. They typically focus solely on the need to detect and neutralize threats, but they generally ignore the need to identify, interrogate, and exploit enemy UASs for important intelligence that can better inform response decisions. For example, understanding the exact purpose of a particular UAS's mission, the details of its payload or sensor package, and the exact type of communications links it relies on will help determine the most appropriate course of action. And if that more granular intelligence can be aggregated with similar intelligence from other UAS threats, it can create a valuable pool of threat intelligence data that reveals broader trends and effective detection and response tactics that can be shared across the military enterprise.

Also, the C-UAS efforts underway today tend to focus on a narrow set of responses to the threat and fail to consider a more complete array of responses for addressing the spectrum of potential threat scenarios. Besides simply destroying or disabling an enemy UAS, other options include overriding it with new instructions; re-directing it to a safe zone; downloading its GPS waypoint plan to better understand its origin and destination; finding the exact location of the UAS's controller; manipulating the intelligence it is gathering to deceive the enemy; and intercepting its video feed to find out what intelligence has been gathered; among others.

In short, a more ideal approach is to create a "networked defense" C-UAS architecture that starts with early detection and responds first with soft deterrence steps to ward off non-threat actors. It then proceeds with interrogative steps to better understand the capabilities and intentions of the UAS, followed by a chain of responses tailored to the specific, evolving threat.

THE COMPLEX C-UAS CHALLENGE REQUIRES AN ENTERPRISE INTEGRATION APPROACH

The current approach of developing a flurry of uncoordinated point solutions to address specific threat scenarios is insufficient for today's dynamic, multi-varied UAS threat landscape. Such an approach hampers interoperability, inhibits technology insertion, diminishes security, and drives up costs with inefficiencies. The complexity of today's fast-evolving UAS threat calls for a more networked approach to the detection, interrogation, exploitation, and response countermeasures needed to address the many scenarios U.S. forces will encounter. A more effective approach requires Enterprise Integration thinking from the outset.

An Enterprise Integration approach to C-UAS starts with an integrated view of the challenge that considers the perspectives of all affected DoD communities, including surface ships, land forces, aviation, facilities, cybersecurity, platform operators, and others. This suggests the need for a single joint office responsible for thinking holistically about the challenge and its many components. A useful model here is Joint Improvised-Threat Defense Organization (JIDO), which began in 2006 as the Joint IED Defeat Organization (JIEDDO) to bring a coordinated, joint-service, enterprise approach to the challenge of IEDs. In consolidating all aspects of capability development into a single organization, JIDO has been widely hailed as a successful model for delivering effective coordination, integration, and increased efficiency to the counter-IED challenge. This notion of leveraging the lessons learned from JIDO to deal with the C-UAS challenge appears to be gathering some support. USSOCOM Commander

Gen. Thomas, while discussing the UAS threat, told lawmakers that "the recent integration of Joint Improvised-Threat Defeat Organization (JIDO) with DTRA [Defense Threat Reduction Agency] provides us with an expanded ability to counter the improvised threats confronting our force today."[6]

An Enterprise Integration approach acknowledges a multitude of conceivable UAS threat scenarios that each require distinct sets of responses and networked defenses. This approach could foster design of an open systems architecture that can accept data from any type of sensor to enable a "plug-and-play" type of approach based on standard interfaces. The result would be a C-UAS system that, depending on the threat scenario, can select from a menu of sensor technologies and response options. A useful model here is the Distributed Common Ground System (DCGS), a cloud-based, open systems architecture based on common interfaces and communications standards that integrates numerous sources of intelligence into a common, real-time operating picture of the battlefield for distribution to multiple military components. Prior to DCGS, military services had to rely on a plethora of disjointed systems to gather intelligence and then manually aggregate those data – a highly time-consuming process – to assemble a full view of the battlefield picture.

Recognizing that simply detecting and neutralizing UAS threats is insufficient, an Enterprise Integration approach incorporates a wider set of options for interrogating, exploiting and responding to enemy UAS threats. This way DoD components have an opportunity to gather and share threat intelligence across the DoD enterprise that can be used to greater effect on the battlefield. A useful analogy here is the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT), which analyzes and assesses cybersecurity threats and vulnerabilities, disseminates cyber threat warning information, and coordinates incident response activities. By taking a similar approach to gathering and disseminating UAS threat intelligence across the military enterprise, DoD planners can ensure that C-UAS capabilities of disparate and far-flung components benefit from the latest known threat intelligence and recommended countermeasures.

As one Army analyst noted: "A common definition of the threat, the establishment of a common threat database, and the establishment of a blue-force positive identification requirement will enhance identification and classification and will help reduce fratricide. In the case of UASs, everything is enemy – until proven friendly. Currently, multiple intelligence organizations are responsible for this mission, and they track fixed-wing and rotary-wing UASs separately. Establishing a common UAS database, with a single intelligence organization responsible for its operation, would provide a considerable advantage for the warfighter."[7]

By adopting an Enterprise Integration model for C-UAS, defense planners can move away from a "gate guard"-type approach to a networked defense system-type collaborative approach that moves beyond the principles of layered defense strategies. The benefits of this are many. An open systems architecture enables the rapid insertion of new technologies while stimulating innovation. It can share and analyze large stores of sensor and intelligence data to better inform C-UAS defense forces in the field. By incorporating multiple varieties of sensor data, it creates a wider aperture to understand the threat more thoroughly for better-informed responses.

Improved insight means research, development and acquisition activities are better coordinated to better leverage scarce resources, ensure that resulting capabilities can be integrated as needed, and avoid duplication of efforts. Cybersecurity is improved because it is designed into the architecture as an organic component. Integrating multiple detection and response capabilities also enables greater resilience when adverse conditions arise. While this approach calls for much greater stakeholder collaboration – horizontally across the services and vertically across strategic, operational and tactical levels – the resulting prioritized requirements and recognition of cross-organizational mission ultimately produce an integrated DoD mindset for the C-UAS mission.

In summary, the C-UAS mission is a vital one that current military service and joint capabilities are struggling to address effectively. By embracing a wider view of the UAS challenge, the Department can gain the advantage in this important arena and thus improve the probability of mission success in the future. An Enterprise Integration approach to C-UAS that relies on joint service leadership and an open systems architecture can produce a robust set of deployable capabilities against a wide array of UAS threats while delivering significant acquisition efficiencies.

NOTES

1. *David B. Larter, "SOCOM commander: Armed ISIS drones were 2016's 'most daunting problem,'" Defensenews.com, May 16, 2017:* https://www.defensenews.com/digital-show-dailies/sofic/2017/05/16/socom-commander-armed-isis-drones-were-2016s-most-daunting-problem/

2. *Caroline Houck, "Trump's Special Ops Pick Says Terror Drones Might Soon Reach the US from Africa. How Worried Should We Be?" Defense One, July 23, 2017:* http://defenseone.com/threats/2017/07/trumps-special-ops-pick-says-terror-drones-might-soon-reach-us-africa-how-worried-should-we-be/139642

3. *Elisa Catalano Ewers, Lauren Fish, Michael C. Horowitz, Alexandra Sander, and Paul Scharre, "Drone Proliferation: Policy Choices for the Trump Administration," Center for a New American Security, June 2017:* http://drones.cnas.org/wp-content/uploads/2017/06/CNASReport-DroneProliferation-Final.pdf

4. *"World of Drones," New America Foundation, April 2015: https://www.newamerica.org/in-depth/world-of-drones/5-non-state-actors-drone-capabilities/ The National Academies of Sciences, Engineering and Medicine, "Owning the Technical Baseline for Acquisition Programs in the U.S. Air Force," 2016:* https://www.nap.edu/catalog/23631/owning-the-technical-baseline-for-acquisition-programs-in-the-us-air-force

5. *Lt. Col. Anthony Tingle, U.S. Army, and 2nd Lt. David Tyree, U.S. Air Force, "The Rise of the Commercial Threat: Countering the Small Unmanned Aircraft System," Joint Force Quarterly, April 2017:* http://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-85/Article/1130654/the-rise-of-the-commercial-threat-countering-the-small-unmanned-aircraft-system/

6. *Gen. Raymond A. Thomas III, Commander, U.S. Special Operations Command, Testimony before the Senate Armed Services Committee, 4 May 2017:* https://www.armed-services.senate.gov/imo/media/doc/Thomas_05-04-17.pdf

7. *Col. Matthew T. Tedesco, U.S. Army, TRADOC Capabilities Manager (TCM) Global Ballistic Missile Defense, Redstone Arsenal, Ala., "Countering the Unmanned Aircraft Systems Threat," Military Review, November-December 2015:* http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20151231_art012.pdf

OUR AUTHORS

Brian Abbe, *Senior Vice President*
Abbe_Brian@bah.com

Troy Abbott, *Distinguished Engineer*
Abbott_Troy@bah.com

About Booz Allen

For more than 100 years, business, government, and military leaders have turned to Booz Allen Hamilton to solve their most complex problems. They trust us to bring together the right minds: those who devote themselves to the challenge at hand, who speak with relentless candor, and who act with courage and character. They expect original solutions where there are no roadmaps. They rely on us because they know that – together – we will find the answers and change the world. To learn more, visit BoozAllen.com.

BOOZALLEN.COM