C4ISRNET

C4ISRNET.com

EDITORIAL WHITEPAPER

Countering the counter-UAS shortcomings

September 2016

A tactical approach to unmanned aircraft system threat response

BY RUTRELL YASIN

Small unmanned aircraft systems are low-cost and readily available, easy to use, and are improving in capability, making them attractive to both hobbyists and commercial industry.

However, those very same attributes make them formidable military tools, giving US forces enhanced capabilities — but also strengthening adversaries as well.

Advanced capabilities enable adversaries to collect data and information to shape military tactics, or send swarms of small drones to distract, disorient, and disrupt military operations.

Such threats, combined with others that thus far remain untapped, have placed counter-UAS efforts at the top of the priority list for defense agencies. It is a key part both of mission strategies and research and development efforts.

And yet, the challenges persist, as unmanned aircraft systems become more advanced and harder to detect, identify, or mitigate.

A significant amount of innovation and improvement in UAS technology is coming from the commercial recreation industry. The sector is driving more and more advanced capabilities into very cheap, small packages offering better optics, communications, data links and navigation capabilities, said Stephen Bramlett with the Army Aviation and Missile Research, Development, and Engineering Center (AMRDEC) at Redstone Arsenal, Alabama.

All of these capabilities present a more complex threat environment for defense, intelligence and law enforcement agencies to counter and avert. It is kind of a cat and mouse game between what the industry is driving for public use versus how adversaries can now militarize commercial-off-the shelf products and use them on the battlefield or against civilian targets, Bramlett said.

"The government, DoD and the Department of Homeland Security are trying to keep up with a commercially competitive-driven hobbyist area of the economy and how that is used now by people with bad intent. It is very hard for us to keep up with that," he said.

Consider the potential harm a small, weaponized UAS with four propellers could cause. In April 2015, a man was arrested in Fukui, western Japan, for landing such a drone on the roof of the Japanese Prime Minister's home. The UAS was carrying a small amount of radioactive sand. The man, 40-year old Yasuo Yamamoto, later turned himself in to police, claiming he landed the drone on Prime Minister Shinzo Abe's roof in protest against the Japanese government's nuclear energy policy.

UASs are essentially flying robots that can be remotely controlled or fly autonomously through software-controlled flight plans working in conjunction with a Global Positioning System.

A UAS consists of an operator, radio frequency signal for navigation and data transfer, payload, and aircraft. UASs are categorized by their maximum takeoff weight, normal operating altitude, and speed. UASs in Group 1 are the lightest, with the lowest operating altitude, and slowest. Group 5 UASs are the heaviest, with the highest operating altitude, and greatest speed.

DoD officials are particularly concerned about UASs with a low-radar cross section and low, slow, and small UAS threats. Older sensors can't detect these vehicles while emerging sensors are often unable to distinguish them from background clutter.

EVOLVING THREAT

Several years ago, adversaries could deploy a quadcopter equipped with a camera for situational awareness, detecting troop movements as well as vehicle and town locations, said David Bessey, director of business development for SRC Inc., a not-for-profit research and development corporation solving problems in the areas of defense, intelligence and the environment.

Currently, adversaries are moving up to higher power, longer range class three UASs that can be weaponized with loaded warheads or with the capability to drop packaged chemical agents, Bessey noted. Enemies don't need the backing of a nation-state to use the inexpensive UAS effectively.

"Part of the evolution is the capabilities of these platforms continues to improve. Battery technology and platform technology are getting more capability; they are faster, have heavier payloads, longer endurance and all of that is challenging as we try to develop requirements for countering them," said Tom Wilson, vice president of business development and product accounts with SRC, Inc.

"Even as we are doing that we are finding the capability has now doubled. We are going to see that for a while," Wilson said.

"There is not one solution that fits all. It is a package of capabilities that combine kinetic and non-kinetic capabilities," Bessey said. The threat is not just one quadcopter running an ISR mission over tree lines, looking at troop positions or a military or base. "It can be a swarm coming from different directions with a combination of ISR and weaponized systems," he said.

Seven Challenges in C-UAS

- Unmanned systems are readily available at low cost, and highly capable.
- Smaller unmanned vehicles are hard or impossible to detect.
- Radar has to find small UAVs amid birds and other clutter.
- Low-altitude UAVs can hide behind buildings and trees to escape detection.
- Determining intent isn't always easy — is the approaching quad copter a threat, or just a toy?
- Mitigation and defeat carries a cost and risks collateral damage.

SOURCE: SRC, INC.

As a result, defense agencies and industry experts are looking at a system of systems approach that incorporates a broad set of capabilities – electronic warfare, electro-optics and infrared cameras, radar and user display, Bessey said.

EFFORTS TO COUNTER THE UAS THREAT

Several of the armed services are exploring technologies to address the growing UAS threat. Most of the initiatives, however, are in the early stages.

AIR FORCE

In April 2016, Air Force Global Strike Command issued a request for proposals for a portable system to counter-UAS systems, or personal drones. The Air Force notes three required steps to C-UAS: Detect, Identify and Defeat. The system should primarily address the defeat portion, but also needs to include the ability to passively detect the radio frequency signature of the UAS or its command and control ground station.

The defeat mechanism must disrupt or manage the control link between a commercial UAS and the pilot. The system should also provide the ability to disrupt the UAS's ability to receive and use satellite navigation signals (both GPS and Global Navigation Satellite System, or GLONASS, Russia's version of GPS) for navigation purposes. The satellite navigation disruption should be engaged with a separate action to allow for different concept of operations, according to the Air Force.

"The system must also passively detect the RF signatures of drone equipment to aid the operator in detecting and locating UASs or their associated ground station. The system must be handheld, portable, and effective across a wide range of UAS targets and not require any separate equipment to operate. The total unit shall not exceed 24 inches in length and must weigh less than six pounds, according to the solicitation.

ARMY

The Army tested a prototype to counter unmanned aircraft systems using capabilities already in the Army inventory at the service's Network Integration Evaluation exercises held at Ft. Bliss, Texas in early May 2016. The NIE is a soldier-led evaluation that assesses how to integrate technology into the Army's tactical network. The evaluation tested how well the C-UAS mobile integrated capability works within the network and how it operates with soldiers. To build its prototype, the Army selected a vehicle already used by the service's fire support teams, the Q-50 counterfire radar system and the lightweight laser designator rangefinder. A defense contractor's telescoping mast system was added to transmit Q-50 radar information and support the LLDR. The Army added SRC's LSTAR software to provide the capability to track air vehicle threats to the Q-50 radar, which traditionally tracks rockets, artillery and mortars.

MARINE CORPS

The Marine Corps Warfighting Lab is working to provide more effective defenses against enemy UAS than an infantry unit's standard small arms arsenal, according to reports in Marine Times. The MCWL work is reportedly focused on Group 1 through 3 UAVs, which current anti-aircraft systems cannot effectively detect, track or attack because of their small size. A group 1 UAV weighs between zero and 20 pounds, and flies lower than 100 feet. Group 3 is a bit larger, and includes the RQ-7 Shadow, which has a wing span of about 13 feet. The AAI RQ-7 Shadow is an American unmanned aerial vehicle used by the United States Army, Marine Corps, Australian Army and Swedish Army for reconnaissance, surveillance, target acquisition and battle damage assessment.

In order to save time, money and reduce the need for additional training, MCWL is considering at least one existing system — the

AN/TPQ-49 lightweight counter mortar radar. Because mortars are small and fast officials think it could also track UAVs and even show their launch location, enabling a strike against the drone or its operators. Additionally, the lab is experimenting with technologies that also include a two-pound nose-mounted radar on a Stalker UAV, which has a 10-foot wingspan. Once they can track UAVs, the next effort is to counter them.

SYSTEM OF SYSTEMS APPROACH NEEDED

AMRDEC's Bramlett thinks a system of systems approach is very much needed to counter-UAS threats. Any end-to-end solution would have to be scalable to the address the geography of the area such as tall buildings or terrain features, he said.

The more important the asset being protected, the more defenders are not going to be satisfied with blind spots, which means investing more money and technology. So there is a balance that has to be considered between the importance of the asset versus the location and the type of approach taken to mitigate the threat, Bramlett said.

For instance, soldiers on the battlefield might be willing to deliver certain effects that defense and security officials would not be willing to do in the Continental US setting, he said. No doubt, though, a system of systems approach in protecting important assets is the approach that defense and military services need to take, he said.

"As threats get more sophisticated, the harder they are to detect and the more technology you have to apply. The biggest thing is it is difficult to afford. That is the biggest problem, trying to afford a solution like that," Bramlett said.

So a cost-effective option is to repurpose existing hardware. At the same time, the military wants to spin in new technologies as quickly as it can that address the threat and politics of the problem. So, flexible acquisition policies and procedures are needed that can be applied government-wide.

For example, re-purposed Army technology plays a part in SRC's Silent Archer anti-drone system, according to SRC's Bessey. SRC is using the Army's lightweight counter mortar radar, the AN/TPQ-50.

The government needs to characterize what the size of the threat is and apply resources to mitigate the threat accordingly. "So you have a quick reaction and the larger government response that is ongoing," Bramlett said.

Government and industry are working together to come up with solutions to counter the UAS threat, he said. "The idea is to try to unite, from the Army's perspective, soldiers, science, technology and industry as quickly as we can to develop a relative near-term solution and let that inform the longer-term solution that is durable."

The Army has been really careful to experiment and test relevant technology with soldiers so officials can find out very quickly what works and what doesn't. That helps the Army determine the requirement process.

TRADOC, the Training and Doctrine Command of the Army, has requirements but they are not always informed requirements. Officials know roughly what they want but they don't know where the edge is, what is the threshold, what is the objective, what is obtainable, or what will take too long to get to the objective, Bramlett explained.

But when industry, science and soldiers are woven together in relevant experimentation, that informs those requirements and they go from being requirements to informed requirements. That gives the DoD a better sense of what can be employed in the near term and what needs to be worked on objectively for the long term.

"We have tried to characterize the threat as best as we can and we are trying to be in the predictive mode of what the threat might be and how to counter those threats and it is not just the threat themselves, it is the tactics," Bramlett said.

"We don't want to take a short term decision and not be able to improve it over time as the threat evolves. We want solutions to evolve with the threat," he said. ■