ASYMMETRIC THREAT SYMPOSIUM XIII
Cyber, Electronic Warfare, and Spectrum Operations: Critical Capabilities for Protecting America
REPORT 3 · SEPTEMBER 2020

Layered Defense for Countering Small Unmanned Aerial Systems

Michael Shields, SVP, Technology and Strategy Implementation, CACI International Inc

Commercial off-the-shelf small unmanned aerial system (sUAS) technologies are ubiquitous, inexpensive, and technically evolving at a rate faster than governments can understand or counter, resulting in constant tactical, operational, or strategic surprise. These small drones are being used for both licit and illicit activities. The accelerating convergence between sUAS and other technologies such as range extenders, autopilot, artificial intelligence (AI)-enabled navigation and autonomy, improved hybrid propulsion, greater payload capacity, and advanced sensors and optics is so rapid and complex that it's challenging for organizations to anticipate and develop effective countermeasures at the speed of relevance. Combined with the threat of networked/synchronized "swarms," the U.S. Government will be challenged in anticipating and matching the technology curve without the private sector's assistance.

Disrupting the "sUAS kill chain" requires **integrated** multi-domain (space, cyber, air, land, and sea), **layered**, and **networked** defense of overlapping long, medium, and short range security measures with redundant capabilities to address sUAS threats that can effectively bypass or manage to survive existing countermeasures.

- Countering adversarial use of sUAS requires a networked, **active and passive**, multi-sensor and effector "system of systems" approach that exponentially increases the speed and probability of detection and defeat, including defeat of non-radio frequency (RF) emitting autonomous drones and swarms.
- A **layered** defense in depth is especially important for wide area coverage because drones are likely to be employed in groups or "swarms" in the future. Therefore, no single defensive layer is reliable enough. A layered approach can help maximize protection based on each system's capabilities and limit the impact of dead space or potential malfunctions. The architecture must provide the threat with both simultaneous and sequential engagement challenges to reduce the likelihood of successful attack.
- Counter unmanned aerial systems (C-UAS) should leverage an open, standards-based **modular architecture** that enables the rapid integration of capabilities.
- C-UAS from national to tactical (of whatever form factor) should be **interoperable** with each other as well as with current and future networks and command and control architectures.

Achieving an effective layered defense will require the integration of AI to help track, locate, and defeat sUAS at "machine speed" (part of the "kill chain"). AI-enabled software will be important in optimizing multiple sensors' capabilities without a human in the loop as well as the fusing of sensor data into a common operational picture to aid in decision making. To counter non-RF emitting drones and swarms, we are going to have to automate or develop a semi-autonomous C-UAS capability to respond at machine speed and lighten the cognitive load on our operators.

There's no one solution to counter the sUAS threat. A layered C-UAS defense needs to take advantage of the **convergence** of electronic warfare (EW), signals intelligence (SIGINT), and cyber, as well as the integration of advanced sensing of multiple phenomenology (with low probability of detection/intercept) with both kinetic and non-kinetic effectors. While there's no silver bullet, a layered defense is one method for countering sUAS threats that are increasingly more autonomous and lethal. ■