March 22 2012

6 Ways to Improve UAVs

After Iran brought down a U.S. stealth drone and in the wake of reports that malware got into the Predator control network, two analysts make the case for aggressively modernizing the U.S. drone force.

by

ROBERT HAFFA and ANAND DATLA

The conditions surrounding the crash landing of a U.S. RQ-170 Sentinel in Iran in December remain murky, but no one doubts that the U.S. lost a highly valued ISR asset. U.S. sources have attributed the loss to a data-link failure coupled with another unspecified malfunction, disputing Iran's claim of hacking into and taking over the drone's computer-guided navigation system. We doubt that these competing claims will ever be resolved conclusively, but of more immediate concern should be the almost cavalier attitude in some parts of the U.S. military over the inevitability of losing unmanned aircraft.

That attitude, recently attributed to an unnamed official within the Sentinel program, is troubling owing to the increased role planned for ISR drones in the future — a centerpiece in Air Force and Navy acquisition plans and budgets. Moreover, the recently released revised U.S. strategic guidance, "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," notes that, in contrast with the last decade, military operations in the future are likely to be conducted in nonpermissive sea and air environments. We believe that if unmanned planes are to continue providing essential intelligence feeds in this new situation, these aircraft must be designed and developed to operate in contested airspace. That means UAVs will need to fly higher, range farther, become less observable and more autonomous, communicate more securely, pull more G's, and protect themselves from kinetic and nonkinetic attacks.

As the guidance suggests, unmanned aircraft strategists must avoid the temptation to think that recent history portends the future. Unmanned air vehicles recently deployed to conduct ISR and strike operations over Iraq and Afghanistan faced few threats from the ground or air. In these uncontested air environments, UAVs proved successful at bringing critical intelligence from an area of interest as well as placing ordnance on targets with great precision. These accomplishments in the field have led to a focus on strengthening sensor capability rather than addressing the challenge of operating in contested airspace. For example, there is currently a substantial effort to enhance data gathered for 12- to 15-hour Predator and Reaper flights. Through technology such as the Gorgon Stare system, UAVs have multiple cameras that capture wide-range images for analysis. Experience with the Sentinel and other UAVs has proved the value of full-motion video to track individuals and vehicles, electro-optical and infra-red cameras used for monitoring missile tests, long-range oblique photography and satellite-communications capability. A byproduct of these sensing improvements has been to build real-time, on-board processing to make imagery immediately available to the war fighter. These efforts have, in turn, created problems, including the challenge of building efficient means to fuse and store data in manageable and rapidly retrievable ways. Operating UAVs in a 24/7 cycle within hostile airspace will add considerably to that challenge.

Regardless of the facts surrounding the Sentinel crash, future adversaries will deploy a number of denial measures to thwart UAVs from entering into and operating within contested airspace. One likely tactic will be to attack UAVs with advanced surface-to-air missiles. Another way to deny access would be to launch fighter aircraft to engage the unmanned vehicle in air-to-air combat. Electronic interference, that is, jamming the aircraft's sensors, will surely be encountered by penetrating or loitering UAVs, while the alleged Iranian tactic, hacking into the UAVs' cyber-control and communications networks, is also plausible. Depending on the sophistication of the adversary, all of these anti-air systems could be tied together into a multilayered integrated air defense system (IADS) enabling long-range acquisition and hand-off to fire control systems. Understandably, past UAV successes while operating in permissive airspace have allowed these challenges to be set aside. But that decade of UAV operations has also provided much to build on in terms of appreciating the contribution of ISR UAVs to situational awareness and, therefore, the need to secure that capability over hostile territory.

The shift of UAVs from uncontested operations to contested air environments has not gone unnoticed at planning levels in the Pentagon. The U.S. Air Force Scientific Advisory Board since the mid-1990s has pointed to the value of UAVs and called for the exploitation of their potential in various roles and missions. In 2009 the Air Force rolled out a "flight plan" focusing on long-term remotely piloted aircraft sensor modernization and integration within budgetary constraints. Last year, the Air Force concluded a summer study intended to inform requests for UAV capabilities for the fiscal 2013 budget and beyond. Reportedly, those challenges included greater integration of ISR across domains and the armed services, and improved methods to fuse information from various UAV-mounted sensors, such as radar, video and signals intelligence.

Most recently, the Joint Chiefs of Staff warned that U.S. competitors are working on strategies and technologies that are likely to make it harder for U.S. forces to operate in key regions of the globe. In their 2012 "Joint Operational Access Concept" document, the chiefs foresee two categories of threats: "Anti-access" capabilities, which are long-range weapons or actions designed to reach far from an enemy's shores, and "area denial" capabilities, which are actions or weapons employed for shorter-range effects. To address the anti-access/area-denial threat, the Joint Chiefs would employ a strategy of "cross-domain synergy," which means compensating for the vulnerabilities of a ship or satellite for example, by being ready to employ aircraft or cyber weapons to achieve the same effect. In the air domain, we believe this strategy implies a family of systems, including unmanned surveillance and strike platforms capable of long-range power projection and sustained operation within contested airspace. The appearance of the Sentinel drone on Iranian TV should serve as a wake-up call to revisit the key issues raised by these studies and to initiate implementation of the most important findings.

How should this wake-up call be answered? UAVs will face a series of competitions in a contested battlespace. In rough order of priority, given desirability, feasibility and acceptability, we offer the following recommendations to help prepare the UAV fleet for operations in future hostile airspace.

- Altitude and range. U.S. fighter pilots have often sought the sanctuary of high altitude to escape ground-based threats, and the same applies to UAVs in hostile airspace. The RQ-170’s operational altitude is approximately 50,000 feet, according to a news report, while the Global Hawk is known to cruise at about 60,000 feet. Depending on the ISR mission, high altitude can provide distinct advantages in fields of view, while providing an additional layer of protection. More powerful engines on the Global Hawk and, perhaps, on other vehicles, could allow higher altitude, increased range and additional electrical power for more numerous and more capable sensors.

- Secure command and control. With all the emphasis on onboard processing to move data off the platform to the battlefield, the loss of communications is a genuine concern. Secure and redundant command and control data links are essential to both offloading high-bandwidth intelligence and ensuring control is maintained over the vehicle at all times, with appropriate fail-safe measures in place in the event of system interference. Satellite communications capability will be required for combat-capable UAVs, and concepts of operation that include “picket lines” of communications relay and “mother ships” to regain control of autonomous vehicles are good fall-back positions when communications with an unmanned vehicle are disrupted.

- Low observability. Stealth, as operators from submarines to the F-22 fighter understand, is a combination of technology and tactics. Therefore, there is room to compromise between high-end, very-low-observable airframes, and reduced signature platforms such as the Sentinel, designed and developed to maximize sortie rates. Nevertheless, based on the mission and the sophisticated sensor suite planned, current UAVs in design and development phases such as the Navy’s X-47B, the MQ-X and an unmanned version of a new long-range bomber must take into account the advantages of very low observability when encountering the forces arrayed to deny access to ISR assets and loitering for long periods within enemy airspace.

- Cybersecurity. The source and effects of a computer virus that reportedly has affected operations of Predator and Reaper drones remain unclear, but what is clear is that UAV ground stations are vulnerable and probably under attack. Cybersecurity for UAVs should be high on the R&D agenda. Those efforts must not only focus on internal communication-navigation system integrity, but also should address the near-real-time availability, accuracy and trustworthiness of ISR data streaming from the UAV. In addition to added cyber protection for assured internal and external information processing, solutions can also lie in variable architecture choices and communications routing options such as UAV-to-UAV, UAV-to-satellite and UAV-to-ground station or airborne relay.

• Electronic defense and attack. Scenarios depicting armed conflict in an anti-access environment frequently feature a “blinding campaign” with the objective of denying the adversary vital ISR information through C2 or sensor jamming. There will be a requirement for UAVs to be able to map the electronic battlefield, update the electronic order of battle, and take both offensive and defensive electronic support measures. Here, UAVs can leverage advances already being made with the next-generation jammer, radar warning receivers, active electronically scanned array radars, and high-power microwave generation, providing the UAV a range of offensive and defensive electronic countermeasures.

• Maneuverability. Unlike manned aircraft, maximum gravitational turns in UAVs are limited only by the strength and life limits of the airframe. There are clear advantages to a double-digit “G” break away from an impending warhead attack that, although probably not a requirement for all penetrating UAVs, could clearly increase the survivability of a drone loitering in a sophisticated IADS environment where multiple layered threats might overwhelm electronic countermeasures. Such design and development could also serve to facilitate UAVs into future offensive counter-air roles and missions.

The recent successes of ISR UAVs in relatively benign environments have led to a focus on sensor payloads and integration more than on their self-protection. Unfortunately, as budgets are compressed, it will be easy to overlook the future challenges of operating UAVs in contested airspace. But the loss of the Sentinel is a harbinger of the future. Addressing some of the recommendations offered here can help ensure this ISR capability is available in the face of growing anti-access capabilities and airspace denial.

Retired U.S. Air Force Col. Robert Haffa directed the Northrop Grumman Analysis Center until 2010. He runs Haffa Defense Consulting, LLC, based in Naples, Fla., and holds a Ph.D. in political science from the Massachusetts Institute of Technology. Anand Datla has worked in strategic planning, policy and operations at the Defense Department and as a professional staff member for the House Armed Services Committee. He is currently a consultant based in the Washington, D.C., area.