Countering the UAS Threat from a Joint Perspective

Lt. Col. Jeffrey Lamport, USAF
Col. (retired) Anthony Scotto, USA

Joint Deployable Analysis Team (JDAT)
Eglin Air Force Base, Florida

BACKGROUND

As technology advances and the U.S. military touts the advantages of drone warfare, other countries, terrorist organizations, and criminals will continue to develop and procure low-cost Unmanned Aerial Vehicles (UAVs). Often, these small, complex systems are equipped with cameras, laser designators, Radio Frequency (RF) collection devices, and/or weapons to provide battlefield intelligence and engage friendly forces. The size and composite materials used in UAV production make them inherently difficult to defeat with traditional force protection measures and Short-Range Air Defense (SHORAD) systems commonly employed by brigade and below maneuver forces.

One of the most significant uses of unmanned systems on the battlefield today is occurring in Ukraine, where both Ukrainians and Russian-backed separatists are operating UAVs in relatively large numbers. They are reportedly operating more than a dozen variants including fixed- and rotary-wing configurations, each functioning at different altitudes with various sensor packages designed to complement each other's capabilities.

The battlefield is not the only susceptible area to the effects of nefarious UAS operators. Our Nation's capital, nuclear facilities, correctional facilities, borders, and sporting venues are among targets already "attacked" with this rapidly proliferating technology. Terrorists leverage UAVs to interrupt our daily routine, while criminals defeat traditional security (e.g., fences, walls, and "no-fly" zones) to scout low-risk routes for illegal alien and drug transport across the border and contraband delivery to prisoners. While these are not traditional military missions, Department of Defense (DOD) specialized equipment and personnel may be tasked to support civil agencies in the Defense Support to Civil Authorities (DSCA) construct.

For nearly 3 decades, the U.S. Army and unified action partners have had the luxury of conducting ground and air operations in a virtually uncontested airspace environment. As such, development and fielding of dedicated SHORAD systems has declined and passive air defense skills have atrophied across the force. Continued UAS technology development, UAS fielding acceleration, and "bad actor" successes around the world clearly demonstrate that we are faced with a viable air threat. Leaders at all levels cannot be lulled into a false sense of security because of the small size of these UAVs. They are as effective, if not more effective, than traditional manned aircraft (or even stealth aircraft) in Reconnaissance, Surveillance, and Target Acquisition (RSTA) precision attack and indirect fire support. Troops must assume they are being watched and targeted and take appropriate action to minimize mission impact.

WHAT LEADERS AND SOLDIERS NEED TO KNOW

UASs can create serious problems for maneuvering or static forces. Their size, composite construction, small radar and electromagnetic signatures, and quiet operation make them difficult to detect and track. Their low-cost, lethality, and rampant proliferation make them an air threat that we can no longer ignore. Some factors contributing to the Counter-Unmanned Aircraft System (C-UAS) challenge are:

a. Small, slow, and low profiles provide significant challenges to traditional air defenses. Conventional systems often "filter" out these tracks to avoid confusion with clutter, large

birds, and aerostats. Systems optimized for this threat often forfeit effectiveness against other target sets (e.g., manned aircraft, cruise missiles, rockets and mortars, and ballistic missiles).

b. Reduction of dedicated SHORAD units to maneuver brigades creates potential gaps in air defense coverage.

c. Soldiers are "numb" to UAVs. Recent combat experience in Iraq and Afghanistan indicates troops may be highly accustomed to friendly UAVs and, therefore, less likely to be concerned about them flying overhead and less inclined to actively search for UAVs operating in their battlespace.

d. Many Soldiers lack UAV recognition training. Without training, it is extremely difficult to observe characteristics visually, which can easily distinguish threat UAVs from friendly systems supporting the mission. This issue is compounded by the ever-increasing proliferation of new UAV designs and off-the-shelf systems sold to multiple countries.

e. U.S. Army and Joint doctrine have not kept pace with the threat.

C-UAS training is not a priority for most units, and many units have not updated plans to address the hazards they present adequately.

UNDERSTANDING THE THREAT

UASs pose a significant threat to safety and mission accomplishment by providing the enemy critical intelligence such as a unit's precise location, composition, and activity. They may also provide laser designation for indirect fires or direct attacks using missiles; rockets; small "kamikaze" munitions; or Chemical, Biological, Radiological, and Nuclear (CBRN) weapons. Some payload configurations can contain radar and communications jamming or other cyberattack technology. UAVs may operate autonomously with little or no RF signature or under pilot control using a Ground Control Station (GCS). The following list describes threat UAS characteristics:

a. Typically comprised of a UAV, a sensor and/or weapons package, GCS, and communications equipment to support navigation and data transfer.

b. Available on the open market, often "clones" of U.S. systems, and cheaper than stealth.

c. Often rely on Global Positioning System (GPS) for guidance/targeting and use multiple RF bands including Frequency Modulation (FM), Ultrahigh Frequency (UHF), Satellite Communications (SATCOM), and cell phones.

d. Small UAVs have a limited range and flight duration, meaning they are frequently operated from within the observed unit's battlespace.

THREAT MITIGATION

Conduct a comprehensive air threat analysis as part of the Intelligence Preparation of the Battlefield (IPB)/Intelligence Preparations of the Environment (IPE) and utilize any resources available to mitigate risks associated with any air threat. Defeating the UAS threat begins with the planning process:

a. Understand the UAS threat. Conduct a deliberate analysis to ascertain the potential UAV type and GCS likely to be employed, understand their capabilities and employment doctrine, predict where and how they will be employed, and identify their most likely targets.

b. Honor the threat. Ensure there are adequate/appropriate resources to counter UAS effects in and around your unit's battlespace. If specialized sensors are not available, be certain to establish "air guards" to scan the airspace continuously. Ensure you understand and are in compliance with the Area Air Defense Plan (AADP).

c. Maintain disciplined flight operations. Although flight clearances for friendly UAVs are sometimes perceived as untimely or overly restrictive, they are critical to ensuring other friendly forces in the area do not engage your UAV. Ensure flights are in compliance with local Airspace Coordinating Measures (ACMs) to aid in proper Identification (ID).

C-UAS CONSIDERATIONS

UAVs are the air threat of the next fight. UAS technology development and employment around the world demonstrates a relevant and viable air threat. Air defense artillery liaison officers cannot be lulled into a false sense of security because of the relatively small size of these platforms. Air defense artillery liaison officers should consider the following when working with/within the Integrated Air Defense System (IADS):

a. Take an active role in AADP development to ensure it adequately mitigates threats to the maneuver force.

b. Suggest UAV-specific Rules of Engagement (ROE) when there is a reliable ability to distinguish unmanned platforms to maximize attrition of low-regret targets. ID and engagement authority for low, slow, small UASs should rest at the lowest possible tactical level.

c. Ensure criteria for "Hostile Act" and "Hostile Intent" specifically address UAVs, are written in terms any Soldier can understand and adequately address ground troop protection.

d. Consider requesting liberal "Hostile" symbology use and ID forwarding through the Air Defense and Airspace Management (ADAM) Cell to the Common Operational Picture (COP).

e. Ensure all Joint data link contributors utilize a common set of track amplification data (i.e., air type, air platform, and air activity) to categorize the UAV target set.

NATIONAL CAPITAL REGION AND INTERAGENCY SUPPORT

Critical assets within the continental U.S. have already been "attacked" by nefarious UAS operators. While no deaths have been attributed to these UAVs, it is only a matter of time before these systems are directly or indirectly responsible for loss of life or interference with critical infrastructure in the homeland. In some circumstances, Title 10 military personnel and equipment may be required to operate subordinate to civil-military organizations, and the following are considerations for working in this environment:

a. Per Department of Defense Directive (DODD) 3025.18[1], DOD resources may be used in an immediate response to prevent loss of life, mitigate damage to infrastructure, or in support of mutual aid agreements (Title 42 USC) to address certain precoordinated conditions or as directed by the President as part of the national response framework.

b. All DOD activity within the homeland is conducted in support of a primary federal agency to minimize impacts to the American people, infrastructure, and environment.

c. It is unlikely that most organic communications systems will be compatible with the civil organization(s) being supported, thereby increasing reliance on knowledgeable liaison officers.

[1] DODD 3025.18, *Defense Support of Civil Authorities*, Change 1, 21 September 2012.

d. Missions may include air defense coverage for the National Capital Region (NCR), key power/communications infrastructure, national borders, sporting arenas, political conventions, and presidential inaugurations.

e. Technology countering the UAS threat within our own borders must be in compliance with existing Federal Aviation Administration (FAA) and Federal Communications Commission (FCC) regulations. Military planners cannot assume they are exempt from fines or prosecution for violating civil airspace or spectrum management policies in the interest of thwarting a potential hazard.

CONCLUSION

UAS development and fielding is gaining momentum with our adversaries, and with each new innovation, they are becoming more capable than the previous generation. We must assume targets of vital interest are being watched and targeted. UAS operations are not limited to the battlefield; they have already been used to disrupt our daily routines at home and violate traditional security measures surrounding our borders, prisons, nuclear facilities, and premier sporting venues. Not all may be traditional military missions; civil authorities will also benefit from our research and analysis, leverage our technology, and request assistance defending airspace around sensitive domestic targets. Leaders across all warfighting functions must take an active role in educating themselves and training their units to defeat this threat.