Everything Old is New Again: Defeating Counter-Unmanned Aerial Systems in the Next War

CW4 Jonas A. Moody, U.S. Army, Air Defense

Air raid sirens blared across cities throughout Israel late in the evening on April 13th, 2024. Israel and its Coalition allies braced for a massive aerial attack from Iran. Drones and missiles were fired from several locations across U.S. Central Command (USCENTCOM) as a "retaliatory strike" for a suspected Israeli attack on the Iranian consulate in Syria that killed two Iranian military commanders and six other Iranian nationals. The attack saw launch points from Iran, Iraq, Syria, and Yemen, illustrating the scope and capability of Iran and its proxy forces throughout the region. Iran's "Operation True Promise" consisted of more than 120 ballistic missiles, 30 cruise missiles, and of particular interest: drones (Al Jazeera Staff, 2024). The drone threat has pushed the Department of Defense (DoD) to act quickly and rush technological solutions to the field. Unfortunately, the rapid acquisition process has resulted in a "throw it at the wall and see what sticks" approach.

Drones, or Unmanned Aerial Systems (UAS) in military parlance, have already changed the face of the modern battlefield, and innovation in the field, both technological and tactical, is proceeding at a ferocious pace. Russia's incursion into Ukraine gave militaries worldwide an unprecedented opportunity to see these technologies employed in the crucible of combat (Thompson, 2024). In addition to the large-scale combat operations (LSCO) unfolding in Ukraine, UAS technology is also changing how the United States conducts counter-insurgency and stability operations across USCENTCOM. At the close of January 2024, three American Soldiers were killed and approximately 34 more were injured when an Iranian-backed militia attacked the Tower 22 outpost in Jordan with one-way attack (OWA) drones believed to be supplied by Iran (Miller, 2024). Unfortunately, this was not the only UAS attack against U.S. forces in the region, but it was the most successful. Frequent drone attacks and incursions on U.S. bases in the region have driven the Department of Defense to flood the theater with rapidly-fielded counter-UAS systems that employ both kinetic and non-kinetic effects. The proliferation of disaggregated systems, contract-driven maintenance programs, and an unfavorable ratio of cost-benefit taxes in existing mission command networks will reduce readiness in LSCO.

Though there is no reasonable way to put a cost on human lives, one must consider the DoD's strategy in how it rolls out these defensive systems. The DoD's response to the emerging unmanned aerial systems (UAS) threat mirrors the disjointed response to the improvised explosive device threat (IED) during the Global War on Terror (GWOT). When IEDs became the threat du jour employed by our adversaries in Iraq and Afghanistan, the DoD rushed to moderate the effects of these low-cost, high-impact weapons and protect American lives. Due to the affordability and high availability of commercial UAS systems, we see a threat similar to the IED, only in the third dimension of the battlespace.

In 2006, the Pentagon created an organization to combat the emerging threat of IEDs called the Joint IED Defeat Organization (JIEDDO) aiming to protect American Soldiers through materiel and training. Martin quotes LTG Michael Barbero (Director of the JIEDDO at the time of her article), "We weren't created to go through some 3- or 4-year acquisition process. We are here to rapidly produce capabilities, and we have been doing that" (Martin, 2011). The U.S. response was to meet the insurgent enemy with an instrument of national power: the economy. Outspending the adversary and leveraging the tremendous intellectual capital of American industry would protect Soldiers and do it faster than the insurgents could innovate. The problem inherent in this solution is economics. Homemade bombs cost less than $50; in 2011, the U.S. spent over $2.8 billion on counter-IED tech. We are doing it again with counter-UAS technology.

However, the first and primary issue with the DoD response to UAS is not economic. The modern doctrine of Operations, Army Field Manual (FM) 3-0, describes the tenets of Multi-Domain Operations (MDO). Of interest to this issue is the tenet of "convergence," which is defined as "an outcome created by the concerted employment of capabilities from multiple domains and echelons against combinations of decisive points in any domain to create effects against a system, formation, decision maker, or in a specific geographic area" (Headquarters, Department of the Army, 2022). Convergence requires integration and interoperability of systems to provide decision-makers with the agility necessary to rapidly analyze and synthesize the battlespace and effectively leverage our technology to achieve effects on the battlefield. Crucial to this effort is the Army Warrant Officer, specialized officers that serve as an "innovative integrator of emerging technologies" (USAWOCC, 2024).

Requisite in that duty description is integrating these disparate systems into the existing mission command structure. Each materiel solution to the counter-UAS problem set produced by the American industry consists of its own vision of how that system should fit into the mission command infrastructure. Inherent in that problem set is the tendency of each service of the DoD to leverage its own existing system profile. We must not forget that the counter-UAS fight is, by nature, a joint fight, requiring unprecedented levels of inter-service integration and interoperability. Unless the services can come to a solution that recognizes the requirement for interoperability across services and echelons, the American Soldiers that implement these solutions on the battlefield, often Army Warrant Officers, will struggle to fit these disparate technologies into the infrastructure that underpins senior leader decision making and will effectively cede the initiative as the Soldiers implementing these technologies grapple with bureaucracy, time, and the complex reality of information systems.

Another crucial role of the Warrant Officer is that of system maintainer. Traditionally, Warrant Officers have served as maintenance leaders, ensuring the various systems under their purview are mission-capable and updated by the latest technical notices. The Soldiers who crew those systems understand preventative maintenance and basic services. As materiel solutions to the UAS problem rush into theater, they often come with warranties or contract logistics support as part of their fielding package. Additionally, since these systems are not yet programs of record, there is no institutional program of instruction to teach Soldiers how to perform critical maintenance functions. This results in a suite of civilian contractors accompanying the system to serve as maintainers and field support representatives (FSR). While this frees up Soldier technicians to focus on other tasks, the requirement to rely upon contract support unduly restricts those same technicians' access to the systems they are responsible for employing in combat. Dunigan writes in a Rand commentary that "[n]ow the U.S. military has developed a growing dependence on private contractors – and for a wide range of functions traditionally handled by military personnel" (2013) and that between 2001 and 2010, contract support cost "nearly $5 billion per year" (2013). During the second quarter of fiscal year 2024, 21,000 contractors were serving in the USCENTCOM theater, with 5,455 personnel performing duties in Syria and Iraq, approximately half being United States citizens (Neenan, 2024).

As the cost to field these systems and the deployment of contractors that support them grows, the adversary continues to find efficiencies that drive down the cost of their weapon systems. While there has been a proliferation of technologically sophisticated UAS created by nation-states to non-state actors and national proxies such as Iranian Aligned Militia Groups (IAMG), commercial off-the-shelf technology can and is weaponized to great effect. Atherton writes about the intersection of commercial technology and military applications when she writes, "while the US-made Reaper drone costs $28 million, the TB2 (a Turkish drone made from commercially available parts) only costs about $5 million" (2023). The TB2 has shown up in conflicts all over the Middle East, Africa, and now Europe. That price tag is still high, considering that drones are available for purchase from Amazon and other internet retailers that sport high-definition cameras and cost a mere $70 to $100. Now, take into account that same drone with a fragmentation grenade duct-taped to its underside. Essentially, we have an incredibly low-cost, low-effort, and potentially catastrophic weapon available worldwide. Contrast these

economical weapon systems with the Department of Defense technology solutions. The Coyote kinetic effector, manufactured by Raytheon, is marketed as a "low-cost rail-launched missile variant… for high-speed Counter-Unmanned Aircraft System missions" (Raytheon, 2024), and they cost $100,000 to $200,000 each. The cost-benefit ratio of using a $100,000 missile to shoot down a $1000 drone is questionable at best.

Unless the Joint Services can come to a shared, economical solution for low-cost UAS defense, the Department of Defense will continue to struggle with meeting the coming ubiquity of UAS on the battlefield. Solutions must be interoperable and, at best, utilize existing programs of record and established protocols defined within military standards (MIL-STD). Those systems should be laboratory-tested for convergence and then proven in Combat Training Centers. Soldiers need to be trained in their employment, and coordinating staff must be aware of the capabilities and limitations of these systems and their tenets of employment and best practices. Warrant Officers and other technician service members must be given the latitude to service and maintain these systems, even if those services are coordinated with FSRs and Contractors. LSCO demands that we think of UAS defense not as a "thing we have to do" but as an integral component of the Protection Warfighting Function, fully integrated into the Operations process. This is a process we need to apply today while we have the luxury of time, for if we wait to react to contact, the UAS threat will be a deadly knife-fight rather than a target we can knock down at three hundred meters.

References

Al Jazeera Staff. (2024, April 15). Iran attacks Israel with over 300 drones, missiles: What you need to know. Al Jazeera. https://www.aljazeera.com/news/2024/4/14/iran-attacks-israel-with-over-300-drones-missiles-what-you-need-to-know

Atherton, K. (2013, January 30). Mass-market military drones have changed the way wars are fought. MIT Technology Review. https://www.technologyreview.com/2023/01/30/1067348/mass-market-military-drones-have-changed-the-way-wars-are-fought/

Headquarters, Department of the Army. (2022, October). FM 3-0 Operations. https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN36290-FM_3-0-000-WEB-2.pdf

Martin, R. (2011, December, 17). The IED: The $30-bombs that cost the U.S. billions. NPR. https://www.npr.org/2011/12/18/143902421/in-iraq-fighting-an-improvised-war

Miller, Z., & Baldor, L. (2024, January 29). Biden says US 'shall respond' after drone strike by Iran-backed group kills 3 US troops in Jordan. Associated Press. https://apnews.com/article/biden-american-service-members-killed-jordan-iran-5cb774fd835a558d840ae91263037489

Neenan, A. (2024, June 6). Defense primer: Department of Defense contractors. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF10600

Raytheon. (2024). Coyote. https://www.rtx.com/raytheon/what-we-do/integrated-air-and-missile-defense/coyote

Thompson, K. (2024, January 16). How the drone war in Ukraine is transforming conflict. Council on Foreign Relations. https://www.cfr.org/article/how-drone-war-ukraine-transforming-conflict

USAWOCC. (2024, January 19). United States Warrant Officer Career College (USAWOCC). The Army University. https://armyuniversity.edu/wocc/courses