

Unprepared for the Unmanned

Addressing the enemy unmanned aircraft threat

by Capt William C. Selby

On the outskirts of the city lies a small island. With only a single bridge providing access from the city, the island is uninhabited and has only a few small structures. The local militants, known to be hostile to the United States, drove off any remaining civilians from the area and now operate out of a single compound near the bridge. As dusk nears, the militants await the arrival of weapons being delivered by a small convoy from the city across the bridge. Off the coast, the MEU is also awaiting the arrival of those same weapons and has an operation underway to intercept the arms delivery to the militants. A forward reconnaissance element lies in wait a few hundred meters away from the compound and monitors the bridge.

After a few hours, the reconnaissance element spots the weapons convoy and alerts the platoon-sized raid force waiting offshore. With the reconnaissance element providing overwatch, the raid force unloads from the Zodiacs and hits the beach undetected. As the raid force nears the compound, its radios are suddenly full of static; despite switching to secondary frequencies, they are unable to reach the command element. Additionally, the reconnaissance element loses radio communications with the raid force while experiencing intermittent communications with headquarters. Overhead, an unfamiliar buzzing sound is barely audible.

Suddenly, a heavy volume of accurate automatic weapons fire halts the advance of the raid force. It quickly attempts to suppress the enemy but is unable to relay its status to higher headquarters without effective radio communications. A few moments later, it is attacked with several mortar rounds. Each round is successively more accurate and it is quickly bracketed.

>Capt Selby is currently completing predeployment training with an advisor team that is due to deploy to Afghanistan this year.

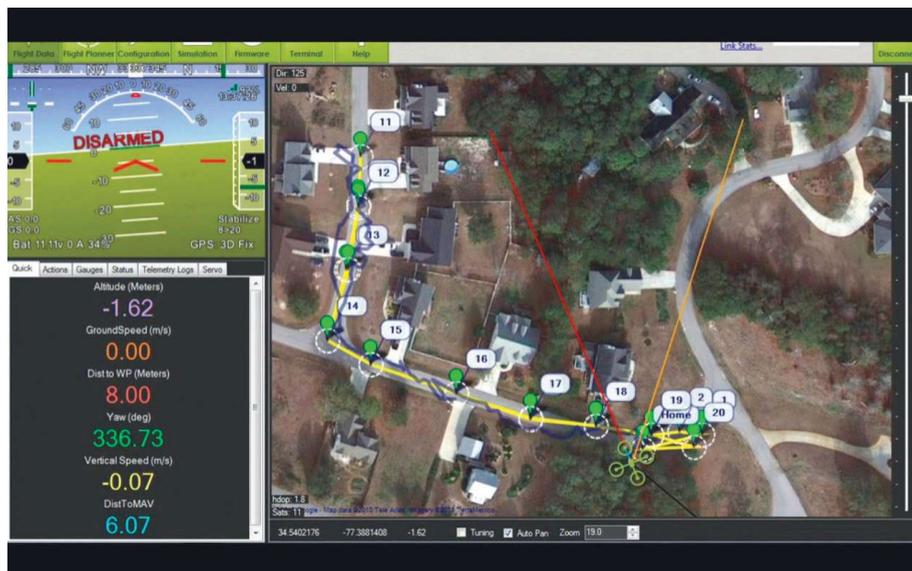
Facing a heavy volume of fire and unable to call for support or extract, the raid team is forced to launch a signal flare and maneuver to the preplanned extraction point. Alerted by the firelight, the enemy weapons' convoy returns to the city to avoid any chance of interception. The MEU commander, alarmed by the loss of radio contact and having seen the signal flare, dispatches transport and attack helicopters to rescue the beleaguered unit. With the attack helicopters overhead, the militants cease firing and the raid force is able to extract safely on MV-22s.

As the raid force heads back to the ship, its members attempt to identify the cause

of their failure. Why did the radio communications suddenly cease? How was the enemy able to target them so quickly and accurately? Unknown to the raid force, a small unmanned aircraft system (UAS) operated by the enemy continues to circle the compound providing real-time video surveillance and electronic jamming capabilities.¹

A New Global Arms Race

While the previous story is fictional in nature, the UAS technologies described therein, as well as the ability for our state and nonstate enemies to acquire and exploit those technologies, are quite real. The scenario demonstrates the potential force multiplier that a UAS could provide the enemy. By attaching a crude thermal camera to a UAS, the enemy was able to detect the presence of the raid force. This in turn gave them advanced warning of the at-



UAS employment is a potential combat multiplier for us and the enemy. (Photo by author.)



Following our example, enemy forces will use UASs to enhance their situational awareness.
(Photo from www.defense.gov.)

tack, allowing them to accurately aim direct and indirect fire from a covered and concealed position. Additionally, the hypothetical militants were able to detect the communications frequencies of the raid and reconnaissance units by using a simple frequency scanner. This enabled them to remotely disrupt communications on those frequencies with a commercially available jammer attached to the UAS. Consequently, by degrading communications and directing accurate fires, the enemy was able to repel the raid force successfully without placing its personnel at risk in an exposed position. Moreover, the enemy was able to accomplish this with little training and a relatively small budget. As this scenario illustrates, the U.S. military and its allies no longer monopolize UAS capabilities. As the technology proliferates, the price to operate a UAS will fall increasingly within reach of even our most technologically unsophisticated enemies.

The threat from an enemy UAS is a real possibility in current and future operations. Our enemies, both state and nonstate, have witnessed the effective use of UASs by U.S. forces in both an intelligence, surveillance, and reconnaissance role, as well as in a kinetic strike role. As such, it comes as no surprise that enemy forces have begun

to utilize their own UASs to provide persistent aerial surveillance at a fraction of the operating cost and with smaller deployment footprints than manned aircraft.² For example, in November 2006, Iranian television broadcast footage of a U.S. carrier in the Persian Gulf that Iran claimed was taken by an unmanned Iranian drone.³

In 2005, there were only 195 drone programs internationally. Today there are an estimated 680 programs, with many countries developing weapon-

In 2005, there were only 195 drone programs internationally.

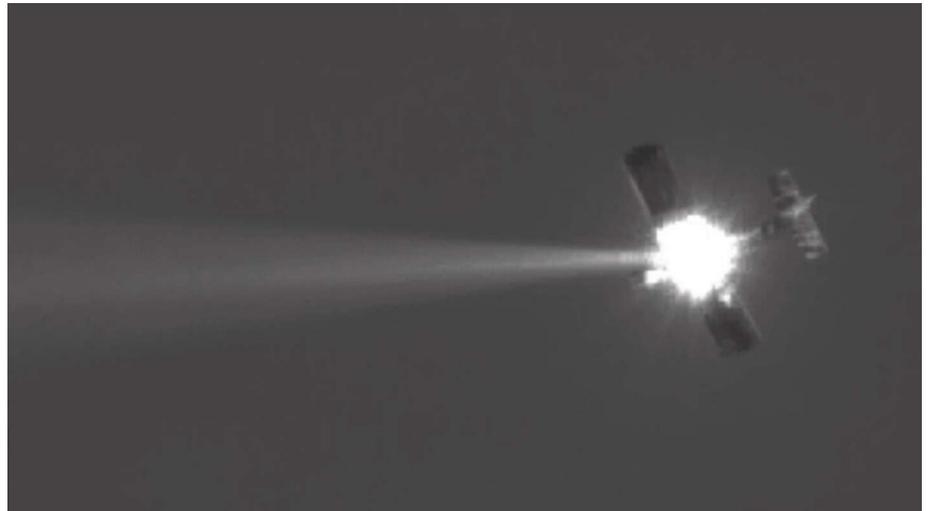
ized versions domestically.^{4 5} As the U.S.'s global military strategy begins to pivot toward the Pacific, it should be noted that in recent years, China has increased UAS research faster than any other country. At its biannual air show last November, China unveiled several UAS models that closely resembled the U.S. MQ-1 Predator and MQ-9 Reaper UASs. The Chinese developers claimed these platforms can be outfitted with common sensors as well as smart

bombs. While the United States has tight export controls on UAS technology, China has made exporting UAS technology a focus.⁶ China is specifically targeting developing countries in Africa, Asia, and Latin America that want short-range UASs that are both portable and low cost.^{7 8} In the immediate future, almost any militant force will have the capability of operating its own UAS.

It should be noted that UAS capabilities are not limited to countries with large research and development budgets and a cadre of engineers. By flying over defensive measures including barriers and fences, UASs allow nonstate actors to attack targets that are difficult to reach with groundbased attack methods. A UAS operation could be launched from a covert location, placing the operator out of direct danger, and has the potential to result in a strong psychological effect on the target.⁹ There are numerous instances of nonstate actors attempting to use UASs. For example, last November, American Rezwana Ferdous was sentenced to 17 years in prison over a plot to blow up the Pentagon and U.S. Capitol using remote-control planes loaded with C-4 explosives.¹⁰ The Colombian insurgent group FARC (Fuerzas Armadas Revolucionarias Colombianas (Revolutionary Armed Forces of Colombia)) possessed multiple unmanned aircraft when a Colombian Army unit overran one of its camps in 2002.¹¹ Perhaps most worrisome, in August 2012, Spanish officials released a video allegedly shot by al-Qaeda showing members training for an attack using a model plane dropping simulated explosives.¹²

If UASs are easy to acquire and provide nonstate actors with a number of advantages, why haven't they been used more effectively? In short, the dynamic exploitation of success is much higher with a simple suicide vest operation compared to a more complex UAS attack. However, the amount of specialized technical knowledge required to ensure a successful UAS operation is quickly falling. For \$1,000, well within the budget of most nonstate actors, it is possible to purchase a low-altitude UAS capable of relaying real-time video foot-

age to a ground station while following a series of preestablished GPS waypoints. Moreover, the knowledge needed to create complex navigation software has been eliminated. A large and supportive online community continually improves open-source software that is both free and widely distributed on the Internet. This software transforms a laptop into a UAS ground control station complete with real-time telemetry and video while allowing the user to send GPS waypoints by selecting the corresponding location on a digital map. Kits that include an aircraft loaded with the required software are available for purchase without revealing the potentially nefarious intentions of the users. While these systems still require users to manually fly the aircraft for takeoff and landing, the limited technical knowledge needed to effectively operate the system is noteworthy. Consequently, the potential expanding threat from UAS requires the Marine Corps to develop



Research programs seek to find groundbased mobile, directed-energy, surface-to-air-weapons for defense of the MAGTF. (Photo from sitere.com.)

the equipment, doctrine, and training to address this quickly emerging threat.

Countering the Unmanned Threat

The 1995 "Report of the Commis-

sion on the Roles and Missions of the Armed Forces" states that the Army is responsible for "groundbased area air defense for all land forces operating beyond the range of naval air and mis-

COMMEMORATE | EDUCATE | SERVE

THE MISSION OF THE MARINES' MEMORIAL ASSOCIATION · SAN FRANCISCO · WWW.MARINECLUB.COM



The non-profit **Marines' Memorial Association** was chartered to honor the memory and commemorate the valor of members of the U.S. Armed Forces who were killed, lost or who died serving their Country.

The Marines' Memorial Club & Hotel is our "Living Memorial," just steps from San Francisco's Union Square. The Club offers 138 air conditioned hotel rooms and suites with broadband access, a health club, library, and rooftop restaurant. Visit our museum, halls with memorial plaques, and our Tribute Memorial Wall. Also, we have 15,000+ sq. ft. of function space for reunions, meetings and conferences.

Veterans and Currently Serving members of the US Armed Forces who join the MMA use the facility at reduced rates, plus have access to over 200 reciprocal clubs worldwide.



CALL (415) 673-6672 OR VISIT MARINECLUB.COM TO LEARN MORE!

609 Sutter Street (next to Union Square), San Francisco, California 94102

sile defense systems,” while the Marine Corps “should retain its low-altitude, ground-based air defense weapons.”¹³ While larger, high-flying UASs can be engaged with traditional air defense assets designed for traditional rotary- and fixed-wing aircraft, the Marine Corps will most likely be on its own for countering low-altitude air threats, arguably the most difficult type of UAS to counter and the type most likely to be acquired with a limited budget. Due to their small size, these UASs are typically battery powered, which reduces their range and payload when compared to larger combustion-powered UASs. Further, UASs’ limited payload makes them hard to employ with any weapons systems more sophisticated than a small explosive charge. Instead, they are typically outfitted with sensors appropriate for an intelligence, surveillance, and reconnaissance role.

Before the enemy UAS can be engaged, it must first be detected, identified, and tracked. The sooner the enemy UAS is detected, the more time the combatant commander has to decide the most appropriate course of action. Low-altitude UASs are small in size, resulting in a limited radar cross-section and thermal signature and making it increasingly difficult for friendly forces to detect and track them.¹⁴ In addition, hostile UASs will not be equipped with identify friend or foe transponders found on friendly aircraft, resulting in airspace deconfliction challenges. Quickly deconflicting the airspace is important not only to accurately classify hostile aircraft, but also to prevent collisions with friendly aircraft operating at similar altitudes.

Fortunately, low-altitude UASs have several distinct vulnerabilities that can be exploited in order to reduce the threat to friendly forces. The relatively short range of the low-altitude UAS makes its launch and recovery sites vulnerable to identification and attack. Additionally, without an escort or a means to detect air-to-air threats, UASs are vulnerable to attack by air assets. Fixed-wing vehicles have shown a history of success despite the challenges that their superior speed creates. For example, two U.S. F-16 fighter jets shot down an Iranian UAS



In November 2012, American Rezwan Ferdaus was found guilty of attempting to use remotely controlled planes loaded with C-4 to blow up the Pentagon and U.S. Capitol. (Photo from esquire.com.)

near Baghdad, Iraq, in early 2009.¹⁵ In October 2012, a UAS launched by Hezbollah was potentially able to transmit images of preparations for a joint Israel-U.S. military exercise before being shot down by an Israeli F-16.¹⁶ Helicopters may be even more effective since they are able to track the UAS at close proximity and match the speed of the enemy aircraft.¹⁷

In areas with increased political or international sensitivity, nonkinetic options may be preferred. Some UASs are heavily reliant on GPS data for navigation and effective sensor operation, making them vulnerable to electronic attack (EA) operations. EA operations directed at the systems controlling the UAS, the UAS itself, or the information downlinks can degrade or deny the ability of the enemy to operate their UAS asset.¹⁸ Spoofing the GPS signal, shown to be technically feasible, requires more specific knowledge about the enemy UAS.¹⁹ Passive actions such as the interception and exploitation of the data collected by the UAS are also possible.²⁰

Preparing a Force for the Future

By analyzing this present threat now, it may be possible to mitigate the effects of surprise as well as develop some basic tactics, techniques, and procedures (TTPs) that can be continually refined in preparation for future counter-UAS-specific platforms. After counter-UAS TTPs have been developed, they need

to be validated in field exercises, and the appropriate units involved need to be trained to proficiency. Enemy UASs are currently incorporated into the Weapons and Tactics Instructor Course exercise scenarios practice that should continue to expand. Enemy UASs need to be incorporated into war games operated by nations, as well as in an asymmetric role operated by non-state actors. Countering enemy UASs should also be addressed in predeployment workups to improve TTPs for air defense units, as well as integrate enemy UAS capabilities and limitations into the planning process. Lessons learned from field exercises such as the annual BLACK DART program or specialized exercises such as BLUE KNIGHT need to be widely disseminated.²¹ Research groups such as the Naval Research Laboratory or Marine Corps Warfighting Laboratory should continue to lend technical expertise to the development of counter-UAS doctrine. Finally, the other Services should refine joint doctrine and share TTPs.

The current generation of UASs will make modifications to improve their defense against both kinetic and nonkinetic weapons. Hardened and alternate navigation systems resistant to GPS jamming and spoofing are in development.²² Future UASs may have their own air-to-air radar to improve their situational awareness and could employ countermeasures found on manned aircraft.²³ Operationally, fu-

ture UASs may be used in groups to allow more efficient use of payloads and may let a single operator control multiple UASs.²⁴

As the world continues to develop UAS capabilities, the Marine Corps needs to develop appropriate countermeasures. The Marine Corps is currently developing mobile platforms to specifically detect and intercept low-altitude UASs, and the Army has looked to the defense industry to provide counter-UAS capabilities for its future forces.^{25 26} The Marine Corps cannot wait for specific systems to be developed to counter low-altitude UASs; instead, the Marine Corps needs to adapt existing planning considerations, training requirements, and TTPs associated with air defense in order to be flexible enough to counter manned and unmanned enemy aircraft in the near-term future. State and nonstate adversaries are acquiring UAS capabilities. These assets will be employed in creative ways that only a prepared force will be capable of defeating.

Notes

1. Department of the Army, *FM 44-100: U.S. Army Air and Missile Defense Operations*, Washington, DC, 15 June 2000.
2. Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, *Task Force Report: The Role of Autonomy in DoD Systems*, Washington, DC, July 2012.
3. *Iran Uses UAV to Watch US Aircraft Carrier on Gulf Patrol*, accessed at www.spacewar.com on 11 November 2006.
4. Wan, William, and Peter Finn, "Global Race on to Match U.S. Drone Capabilities," *The Washington Post*, Washington, DC, July 2001, accessed at www.washingtonpost.com on 4 July 2011.
5. Zenko, Micah, *The Coming Future of Autonomous Drones*, Council on Foreign Relations, Washington, DC, 4 September 2012.
6. McDonald, Mark, "Growth in China's Drone Program Called Alarming," *The New York Times* blog, accessed at rendezvous.blogs.nytimes.com on 27 November 2012.
7. Beckhusen, Robert, "China unveils its new drone fleet to the world," *Wired*, accessed at www.wired.co.uk on 28 November 2012.
8. Hsu, Kimberly, "China's Military Unmanned Aerial Vehicle Industry," *U.S.-China Economic and Security Review Commission Staff Research Backgrounder*, Washington, DC, 13 June 2013.
9. Miasnikov, Eugene, *Threat of Terrorism Using Unmanned Aerial Vehicles: Technical Aspects*, Center for Arms Control, Energy, and Environmental Studies at Memorial Institute for the Prevention of Terrorism, Dolgoprudny, Russian, June 2004.
10. Bidgood, Jess, "Massachusetts Man Gets 17 Years in Terrorist Plot," *The New York Times*, accessed at www.nytimes.com on 17 July 2013.
11. "Colombia-FARC Drones Discovered," *EFE News Service*, 28 August 2002.
12. El-Shenawi, Eman, *Toy Planes and Miniature Bombs: How al-Qaeda Plots Terror*, accessed at english.alarabiya.net in August 2012.
13. Department of Defense, "Report of the Commission on the Roles and Missions of the Armed Forces," Commission on the Roles and Missions of the Armed Forces, Washington, DC, 1995.
14. U.S. Army, *FM 44-100: U.S. Army Air and Missile Defense Operations*, Washington, DC, 15 June 2000.
15. "U.S.: We shot down Iranian drone over Iraq," CNN, accessed at www.cnn.com on 16 March 2009.
16. "Hezbollah UAS Took Pictures of Joint Israel-U.S. Military Exercise," *UAS Vision*, accessed at www.uasvision.com on 16 October 2012.
17. Headquarters Marine Corps, *Marine Corps Warfighting Publication 3-42.1, Unmanned Aerial Vehicle Operations*, Washington DC, 2003.
18. Headquarters Marine Corps, *Marine Corps Warfighting Publication 3-42.1, Unmanned Aerial Vehicle Operations*, Washington, DC, 2003.
19. "Drone hack explained: Professor details UAV hijacking," RT.com, accessed at rt.com on 3 July 2012.
20. Office of the Secretary of Defense, *UAS Roadmap 2005-2030*, Washington, DC, 4 August 2005.
21. Kenyon, Henry, "Military refines techniques to counter hostile drones," *Defense Systems*, Falls Church, VA, 16 August 2011.
22. "Rockwell Collins Launches Real Time Kinematic Anti-Spoofing Technology," *UAS Vision*, 14 August 2012.
23. Kenyon.
24. Freedburg, Sydney, Jr., "Drones Need Secure Datalinks to Survive vs. Iran, China," *AOL Defense*, 10 August 2012.
25. Headquarters Marine Corps, Deputy Commandant, Combat Development and Integration, *2012 Marine Corps S[cience] & T[echnology] Strategic Plan*, Washington, DC, 2012.
26. "U.S. Army Issues RFI for Counter-UAS Technology," *UAS Vision*, Washington, DC, 26 September 2012.



Blended Seminar Program



**Expeditionary Warfare School
Command and Staff College**

Contact Your Regional Director

www.tecom.usmc.mil/cdet
1.888.4DL.USMC