Embrace The Hive

Loitering munitions and UAVs

by Capt Fabio Garcia & Mr. Patrick Griffin

>Capt Garcia is a Naval Aviator with experience in Marine Corps unmanned aerial vehicle tactics, as well as fifth-generation fighter employment. Having been a part of joint deployments and exercises, he has a unique perspective on the modern-day battlefield. He holds a degree in Systems Engineering from the United States Naval Academy and is stationed in Yuma, AZ.

>> Mr. Griffin is a Marine Corps veteran and current graduate student at Harvard University, Extension School, working towards a master's degree in International Relations. He holds an undergraduate degree in International Affairs from from Florida State University and enjoys reading and writing on international relations and national security topics.

Loitering munition devices like the Switchblade are proving themselves as effective new tools for Ukrainian armed forces in their fight against Russia.[1] The Marine Corps is looking for its own loitering munition variant to adopt and integrate into the MAGTF.[2] Integrating multi-platform command and control (C2) for these devices will increase their resiliency, lethality, and flexibility. This will transform the traditional kill chain into an interconnected web that supports mosaic warfighting theory.[3] Loitering munitions (LM), launched by Marines on the ground need the capability to link with medium or high-altitude long-endurance drones to guide them and coordinate the final flight-to-target. This article references the MQ-9 Reaper because it is the main effort of the Marine Corps' unmanned aviation program. Expanding the current kill chain of LM into a web of mutually supporting assets increases battlefield flexibility, speed, lethality, and economy of force while reducing risk and uncertainty. Leveraging semi-autonomy, artificial intelligence, and machine learning further expands LM capabilities. Finally, redundancies in communication prevent interruption in the kill web, so that when one node of control is interrupted or offline another can take its place. All this works to present a vision for 2030, a vision that embraces the hive.

Increased Flexibility, Speed, and Lethality

Third-party management of loitering munitions post-launch enables a Marine infantry squad to focus on closing with and destroying the enemy, revolutionizing the concept of fire and forget. Reaper crew management of the LM orbit and impact generates greater flexibility for ground units. This flexibility creates opportunities to adopt new tactical procedures that will increase speed and lethality. For example, a team has the option to launch loitering munitions with a specific target in mind and conduct a full infiltration and extraction. During which, the LM is used as an instant close air support (CAS) munition under the control of the Reaper team. Ground forces may also launch multiple loitering devices, then time their strikes in phases, or as a swarm in coordination with maneuvers on the ground. This cheap, scalable, flexibly functional design yields itself to mosaic warfighting championed by the Defense Advanced Research Project Agency. This theory is designed to challenge traditional methods of using expensive monolithic systems that suffer from single-purpose use as part of a *jigsaw puzzle approach* to military operations.[4]

Instead of carrying a finite amount of conventional ordnance, creating a kill web of loitering munitions can provide the MQ-9 with a supply of explosives limited only by how much each unit in the battlespace can carry. Loitering munitions are a unique capability, since no missile can loiter once fired and wait for its target to re-emerge from a building or bunker. For example, if an intended target hides behind walls, or in a specific room in a building, a pilot delivering a Hellfire missile will undoubtedly lose the line of sight needed to consummate the kill. This is where the LMs, capable of relaying a feed to an overwatch MQ-9 or a squad leader on the ground, would be able to deliver the payload to its desired point of destruction. In other words, if a target moves behind cover, a loitering munitions round is capable of circling until the target becomes available again.

Decreased Risk and Uncertainty

One lesson learned comes from Ukraine's special drone unit, *Aerorozvidka* (which utilizes a combination of LMs and off the shelf drones). In a report from the *Guardian*, a spokesperson for the unit claims, "The Russians can latch on to the drone's electronic signature and quickly strike with mortars, so the Aerorozvidka teams have to launch and run."[5] To mitigate this risk, teams launching the LMs can relinquish control to the MQ-9 preventing opportunity for counterstrikes to the ground units. Ground units are not the only ones to benefit from the risk mitigation of this tactic. A 2014 report on combat airpower said, "With the exception of a small number of stealthy F-22s and B-2s, DOD's fighters and

bombers have lost their ability to operate in high-threat areas without the risk of significant losses or the need for very large supporting force packages to suppress enemy air defenses."[6] Loitering munitions can conduct strikes on ground targets in these highly contested areas without the risk of losing valuable aircraft and pilots.

Interfacing the MQ-9 with loitering munition devices allows for greater battlefield integration. Communication between multiple loitering devices, all flying within the reception of a single MQ-9, clarifies the battlefield picture for every unit patched into the video feed. Relaying video feeds through the MQ-9 shares more battlefield information to commanders, other operators, and higher headquarters. This culminates in a clearer overall picture of enemy movements and concentrations. Creating a better visualization of enemy concentrations reduces the fog of war and reveals which gaps to attack as well as what surfaces to avoid. Finally, watching live streams of loitering munition strikes via an MQ-9 link supplements battle-damage assessments, streamlining battlefield communication.

Economy of Force

Loitering munitions can adjust their payload to meet the appropriate scale of their target. In the future, a standard Marine Corps weapons company can carry launchable LM packages designed for a variety of targets. This variety gives the end-user the ability to match the appropriate ordnance to target. Doing so will prevent a disproportionate use of force that has long plagued the U.S. military. For example, the United States originally developed the Hellfire as an antitank weapon in the 1970s.[7] However, over time this $71,000–$150,000 missile took on a multipurpose role, to include targeting individual enemy combatants.[8] Using a $6,000 Switchblade to kill an enemy combatant with only $1,000–$2,000 worth of equipment is a far more proportional response.

The Switchblade 300 is one of the current loitering munition drones supplied by the United States and used in Ukraine.[9] The estimated $6,000 cost of each Switchblade[10] is significantly lower than a $78,000 Javelin missile,[11] $40,000 Next Generation Light Antitank Weapon missile,[12] or $71,000–$150,000 hellfire missile.[13] By utilizing single-use drones we can achieve low collateral, lethal effects for approximately one-twelfth the cost of weapons we currently use.

A U.S. Marine Corps Hero-400 loitering munition drone a loitering munition that the United States Marine Corps is beginning to incorporate into specific mission sets. ***(Photo by LCpl Daniel Childs.)***

The current cost to operate aircraft such as the F-15, F-16, F/A-18, and F-35 runs at approximately $23,000–$38,000 per flight hour per aircraft.[14] Each time one of those fighters launches to support troops on the ground in the role of a CAS platform, they will spend anywhere from six to eight hours airborne. After traveling hundreds of miles, dragged along by a tanker, each fighter can only remain on station for an average of $1^{1}/_{2}$ hours until it needs to refuel. This creates potential gaps in coverage. Furthermore, these platforms never operate alone, fighting in teams of at least two or more, thus doubling or tripling their cost per hour.

Meanwhile, an MQ-9 with the extended range configuration, like the model purchased by the Marine Corps, will be capable of staying airborne for up to an advertised 27 hours without constantly leaving to refuel.[15] With a cost of $5,000 per flight hour and the ability to stay on station for over eighteen hours (transit time not included), the MQ-9 is an obvious choice for a CAS platform. Let fighters be fighters and establish air dominance. Critics will say that the Reaper may not have the weapons necessary to be considered a strong CAS aircraft, but that is where teams of small unmanned aircraft systems (SUAS), and other loitering munitions working in unison with the MQ-9 can make all the difference.

Finally, cost must also be considered in combat losses. The loss of unmanned aerial drones, even those at the larger scale like an MQ-9, are still significantly lower than the cost of any piloted aircraft. The costs fall even further when MQ-9's are delivering secondary SUAS onto targets, and the highest risks are therefore assumed by the cheapest assets. This is not the case with traditional CAS where pilots assume all the risk by carrying out these missions themselves.

Semi-autonomy, Artificial Intelligence, and Machine Learning

To manage a sortie of smaller drones, an MQ-9 pilot must leverage semi-autonomous flight. Artificial intelligence is the solution for co-piloting multiple loitering drones, freeing the UAV operator for only the most critical tasks like

final strike approval. Deconflicting aircraft, target identification, coordinating swarm formations, and designing flight paths to confuse or avoid enemy radar detection are all roles for an artificially intelligent co-pilot.

Drone swarms can be tailored to fit endless scenarios using image recognition and artificial intelligence to create pre-selected target collection lists and then send those lists to a swarm. For example, to destroy aircraft on an airfield without damaging the infrastructure, the swarm receives AI-identified and generated coordinates to the locations of each parked aircraft. Then, analyzing the size of the targeted aircraft, these loitering munition drones could carry out attacks individually, or swarm together to destroy larger airframes. This same strategy is adaptable to a wide array of potential targets, like ports housing fast ingress attack craft, that are becoming very popular in countries like China and Iran.[16]

Companies like Palantir provide the means to achieve an advantage over the enemy and maintain the initiative through products such as Gotham.[17] This application enhances user decision making through sensor fusion information, augmented by machine learning algorithms. For example, targeting and weaponeering could easily be achieved during a live flight based on the munitions available throughout the battlefield, not just what a single platform is carrying. For LM and Reaper teams, apps like Gotham could help crews determine how many loitering munitions should be launched prior to the battle and how many will be required to destroy a certain target. Information that at one point in history was left to teams of weaponeering experts to derive, many days before a battle, with outdated information.

Because all strikes from loitering munitions are recorded over an array of video and other sensors, machine learning should assist in post-strike analysis. As a conflict matures, adversaries will learn and adapt to even the most reliable tactics. Machine learning of post-strike analysis is an efficient way of detecting these adaptations and analyzing trends among successful and unsuccessful strikes. Transforming the traditional kill chain between a drone operator and device, into a web of shared information and control, maximizes the opportunity for learning and adaptation from post-strike analysis.

Communication Redundancies

Interception of radio transmission through jamming is a common countermeasure for remote-piloted drones.[18] To circumvent this vulnerability, operators can launch loitering munitions with pre-packaged downloadable data. Once this device is able to make a connection, the MQ-9 targeting data can tell the operator all they need to know about the strike mission without needing to communicate with operators on the ground. Similarly, instructions from the MQ-9 can be sent via a small download package containing final instructions instead of maintaining a continuous connection. Pre-set instructions in the munition software can contain abort instructions that disarm the ordnance if the device identifies specific civilian or other collateral criteria on its final approach.[19] This technology limits civilian casualties, a major critique of current drone strikes, in a way that is impossible for a Hellfire or similar ordnance.

If an MQ-9 is unavailable to pilot loitering munition, the option for manual piloting can leverage civilian cellular networks. Instead of connecting to loitering munition via a radio frequency that can be traced back to its user, Ukrainian forces have successfully hidden their connection within the mask of civilian cellular traffic.[20] Furthermore, recent research suggests that LTE connections can provide "'essentially unlimited operation range,' making the pilot harder to find."[21] A report on UAV countermeasures also states that "LTE drones would be difficult or dangerous to interdict with jamming systems without interfering with ubiquitous cellular communications."[22]

Finally, it is important to note that Ukraine relies heavily upon Elon Musk's private company providing internet service—Starlink.[23] While outsourcing this capability allows Ukraine access to competitive high-end communication, it does not come without vulnerabilities. Recent Twitter announcements from Elon Musk, wavering over whether or not to continue to provide service, reveals the vulnerability of outsourcing a critical asset.[24] This instance reveals the importance of leveraging critical communication connection and security through joint-force cooperation with the Space Force. Doing so protects forces from friction between private companies and the U.S. government and unburdens internal organizations like Marine Corps Cyber Command from creating and managing cyber infrastructure themselves. Establishing secure connections for ground units to pilot loitering launched munitions creates resilience in the kill web so that if one strand is broken, the rest of the web survives.

A Vision of 2030

In 2030, the People's Republic of Centralia began capturing island nations throughout the South Centralia Sea claiming that it was time for them to rejoin the Republic. Some of those nations had agreements with the United States that they would receive military support in case the Centralians moved against them. Fast forward a few months and the Marines began launching long-range air strikes from amphibious ships. The combination of fourth and fifth-generation fighters was successful in cleaning up the air picture enough to create a permissible environment in which unmanned aerial vehicles could operate. The medium altitude long endurance MQ-9 with a versatile suite of payloads is perfectly suited for the next portion of the campaign, clearing the beachhead enough for the GCE to arrive.

The plan is to launch the MQ-9s and have them loiter outside of potential weapons engagement zones and develop patterns of life on the island nations. They will also be tasked with gathering signals intelligence, helping to generate a picture of the battlefield ahead of the forces. However, their primary job will be to locate enemy forces on the ground and relay that information, via secure tactical data link networks to swarms of SUAS and LMs. These SUAS have

varying payloads and are waiting to be launched off the amphibious ships. With targetable coordinates in their system, the swarms will then close with and destroy the enemy forces protecting the beaches and potential MV-22 landing zones with surgical precision. This is achievable thanks to the weeks of non-kinetic attacks in the cyber realm. Attacks aimed at bringing down enemy lines of communication and disabling networks that enable the Centralian integrated air defense systems to operate harmoniously.

As the landing forces make their way inland, teams of Marine Raiders will begin to infiltrate farther behind enemy lines to collect intelligence and strike critical command, control, and communication nodes. MQ-9s will be up and on station for the entirety of the special operations thanks to their long endurance, scanning the battlefield for possible threats. To preserve its life, the MQ-9 it will have to operate outside of suspected surface to air threat weapons engagement zones. By doing so, the MQ-9 will be denied the ability to launch air-to-ground missiles because of their limited range. On the ground, the Raiders will launch LMs at different portions of their mission with the sole purpose of receiving targetable data from the MQ-9 loitering so many miles away. As the Raiders close in on their objective, the MQ-9 will use sensors to locate enemy forces. Quickly coordinating with targeting cells and the team on the ground the MQ-9 sends the Centralian's locations to the loitering munitions launched by the Raiders and the enemy is destroyed in a matter of minutes. The kill chain has been significantly reduced and the Marines are able to carry on and complete their mission, thanks to the new way to perform CAS.

Notes

1. Andrew Eversden, "'Bigger, Faster, Longer': As Market Grows, Loitering Munition Makers Eye Next Evolution," *Breaking Defense,* July 21, 2022, https://breakingdefense.com/2022/07/bigger-faster-longer-as-market-grows-loitering-drone-makers-eye-next-evolution.

2. Hope H. Seck, "As Ukraine Highlights Value of Killer Drones, Marine Corps Wants More," *Marine Corps Times,* August 11, 2022, https://www.marinecorpstimes.com/news/your-marine-corps/2022/08/11/as-ukraine-highlights-value-of-killer-drones-the-marine-corps-is-asking-for-more.

3. BAE Systems,"What is Mosaic Warfare?" *BAE Systems*, n.d., https://www.baesystems.com/en-us/definition/mosaic-warfare.

4. Benjamin Jensen and John Paschkewitz, "Mosaic Warfare: Small and Scalable are Beautiful," *War on the Rocks,* December 23, 2019, https://warontherocks.com/2019/12/mosaic-warfare-small-and-scalable-are-beautiful.

5. Julian Borger, "The Drone Operators Who Halted Russian Convoy Headed for Kyiv," *The Guardian*, March 28, 2022, https://www.theguardian.com/world/2022/mar/28/the-drone-operators-who-halted-the-russian-armoured-vehicles-heading-for-kyiv.

6. Mark A. Gunzinger and David A. Deptula, *Toward a Balance Combat Air Force*, (Washington, DC: Center for Strategic and Budgetary Assessments, 2014).

7. Matt Gluck and Masao Dahlgren, "Hellfire | Missile Threat," *Missile Threat*, April 23, 2024, https://missilethreat.csis.org/missile/agm-114-hellfire.

8. Ibid.

9. Hannah Fuchs, "Drones Are Changing Modern Warfare," *DW,* April 5, 2022, https://amp.dw.com/en/ukraine-how-drones-are-changing-the-way-of-war/a-61681013.

10. Ken Dilanian, "Biden Admin Will Provide Ukraine Killer Drones Called Switchblades," *NBC News*, March 15, 2022, https://www.nbcnews.com/politics/national-security/ukraine-asks-biden-admin-armed-drones-jamming-gear-surface-air-missile-rcna20197.

11. Inder S. Bisht, "Lockheed Martin to Ramp Up Javelin Production," *The Defense Post,* May 3, 2022, https://www.thedefensepost.com/2022/05/03/lockheed-ramp-up-javelin-production.

12. Peter Suciu, "Javelin vs. NLAW: Which Missile Is Better at Destroying Russian Tanks?" *19FortyFive*, February 23, 2023, https://www.19fortyfive.com/2022/05/javelin-or-nlaw-which-missile-is-better-at-destroying-russian-tanks.

13. Staff Writer, "AGM-114 Hellfire Missile Ultimate Guide: Capabilities, Variants, and Cost," *The Defense Post*, March 22, 2021, https://www.thedefensepost.com/2021/03/22/agm-114-hellfire-missile.

14. Sebastien Roblin, "The Air Force Wants to Cut Surveillance Drones—Here's Why That May Be a Mistake," *Forbes,* April 20, 2020, https://www.forbes.com/sites/sebastienroblin/2020/04/20/the-air-force-wants-to-cut-surveillance-drones-a-think-tank-argues-thats-a-mistake/?sh=4e4b4b714e69.

15. General Atomics Aeronautical, "MQ-9A Reaper (Predator B)," *General Atomics Aeronautical Systems*, n.d., https://www.ga-asi.com/remotely-piloted-aircraft/mq-9a.

16. Dave Makichuk, "China Deploys Fast-Attack Missile Catamarans in SCS," *Asia Times*, April 10, 2021, https://asiatimes.com/2021/04/china-deploys-fast-attack-catamarans/; and United States Navy Press Office, "Unsafe and Unprofessional Interaction with Iran's Islamic Revolutionary Guard Corps Navy," *Navy.mil*, April 27, 2021, https://www.navy.mil/Press-Office/Press-Releases/display-pressreleases/Article/2586021/unsafe-and-unprofessional-interaction-with-irans-islamic-revolutionary-guard-co.

17. Palantir, "Palantir Gotham for Defense Decision Making," YouTube video, 5:19, June 8, 2021, https://www.youtube.com/watch?v=rxKghrZU5w8.

18. Arthur Holland Michel, *Counter-Drone Systems,* (Red Hook: Center for the Study of the Drone, 2019).

19. Business Insider, "The True Cost of Killer Drones," Youtube video, 11:45, August 16, 2022, https://www.youtube.com/watch?v=8MapFmEnDa4&t=17s.

20. Center for Strategic & International Studies, "Assessing Russia's War in Ukraine," YouTube video, 58:54, June 16, 2022, https://www.youtube.com/watch?v=CzbsPOaCrLw.

21. *Counter-Drone Systems*.

22. Ibid.

23. BBC, "How Are 'Kamikaze' Drones Being Used by Russia and Ukraine?" *BBC*, December 29, 2023, https://www.bbc.com/news/world-62225830.amp.

24. Shubham Kalia, "Musk Says SpaceX Cannot Fund Ukraine's Vital Starlink Internet Indefinitely," *Reuters*, October 14, 2022, https://www.reuters.com/technology/musk-says-spacex-cannot-fund-ukraines-starlink-internet-indefinitely-2022-10-14.