Industry Insights Brief

FORECAST INTERNATIONAL

New-Age High-Power Microwave Technology:

A Strategic Countermeasure in Asymmetric Drone Warfare

Introduction

Unmanned aircraft systems (UAS), commonly referred to as drones, have undergone a lightning-fast evolution into accessible, affordable, and capable weapons. Agile, cost-effective, and equipped with the latest technology, drones have quickly become a popular asymmetric tool on the battlefield. Recent Houthi attacks on shipping vessels in the Red Sea and the ubiquitous presence of drones in the Russia-Ukraine conflict have demonstrated the democratization of drones across state and non-state actors and put a premium on robust, versatile, and cost-efficient counter-drone (C-UAS) solutions. This brief will detail why C-UAS is so critical, list the C-UAS solutions available today, explain how each works, identify their drawbacks, and determine the most effective C-UAS solution.

Defining the Threat

UAS Proliferation and Ubiquity

Militarized drones have quickly been adopted by militaries, non-state actors, and individuals across the globe, effectively allowing any nefarious actor to develop a menacing and often lethal air presence. Moreover, the intelligence, surveillance, and reconnaissance (ISR) capabilities of drones have created an unprecedented level of transparency on the battlefield. The proliferation of drones and their ISR capabilities have made it easier to find and target centralized, expensive platforms. This has contributed to a larger strategic shift in warfare toward more distributed, attritable systems. Additionally, thanks to their efficiency, accessibility, low cost, and evolving sophistication, drones have become commonplace on the battlefield and will remain a persistent and growing challenge for the foreseeable future. Therefore, the U.S. must carefully consider which C-UAS solutions it employs to protect critical infrastructure at home and warfighters and allies abroad from this evolving threat.

Cover Image: Adobe Stock | sandsun

Key Challenges

A Variety of Evolving Threats

Driven by commercially-led innovation, drone manufacturing has exploded in recent years. This has resulted not only in a torrent of these capabilities onto the battlefield but also in a diversity of drone types with unique defense considerations. The Defense Department categorizes drones into five different groups, with Group 1 representing very small drones like quadcopters and Group 5 designating the largest drones, like an MQ-9 Reaper.[1] Military leaders and policymakers making difficult decisions about C-UAS solutions must consider domain-specific problem sets and the protection of diverse and distributed targets, including critical infrastructure, military installations, vehicles, naval vessels, and dismounted warfighters. Additionally, decision-makers need to consider how to secure a more enduring advantage in C-UAS solutions, shifting out of the move-countermove cycle as UAS developers seek novel ways to harden and inject self-protection capabilities into their drones.

Drone Swarms

Drones, when launched en masse toward a target, present a distinct challenge. A swarm of dozens of agile drones attacking simultaneously from multiple directions can easily overwhelm traditional air defenses that are not well-equipped, nor designed, to neutralize this type of attack. These “drone swarms” are no longer a concept of science fiction and have proven difficult for even the most robust C-UAS solutions. At present, China possesses a swarm launcher that can fire 18 drones at once.[2] Technological advancements in AI, communications networking, and edge computing will make swarms even more sophisticated as militaries experiment with true cooperative autonomy. Some experts predict future scenarios in which hundreds, or even thousands, of drones engage in coordinated battle.[3] This new threat necessitates C-UAS capabilities that are designed to defeat several drones at once (i.e. moving beyond a 1:1 kill ratio) without traditional kinetic magazine limitations.

iStock | Chesky_W

Inefficiencies of Traditional Munitions

Using traditional air defense, such as missiles, to destroy drones presents an obvious challenge. Larger munitions can cost far more than the relatively inexpensive drone they target and are more difficult to procure. This cost imbalance is clearly illustrated by recent attacks in the Red Sea in which expensive surface fleet weapons have been expended to take out cheap one-way attack drones fired by Houthi militias. Since December 2023, the U.S. Navy has used over $1 billion worth of munitions knocking threats out of the sky and out of the water.[4] With limited ammunition, traditional air defenses can be exhausted by cheap drones, leaving them vulnerable to more strategic threats such as enemy aircraft or missiles. Therefore, C-UAS solutions must be both cost-effective in relation to the value of the target and have deep magazines without compromising efficiency.

Another major drawback for traditional munitions is that component shortages exacerbate already strained production lines for air defense systems, causing multi-year-long delays in production and delivery. A global scramble for missiles has meant it now takes around two years or more to deliver some air-defense interceptors. For example, the National Advanced Surface-to-Air Missile System (NASAMS) takes two years to manufacture and there is already a multiyear backlog.[5] Other missile categories have similar issues. In 2023, Lockheed Martin and RTX reported that doubling production of Javelin and Stinger surface-to-air missiles will take four years, twice as long as expected, due to supply-chain challenges.[6] Given the limited supply of these costly missiles, their strategic use becomes all the more valuable. Launching multiple missiles at a drone swarm, for example, would be an extremely costly countermeasure.

Adobe Stock | GustavsMD

Overview of Contemporary C-UAS Technologies

Military leadership is acutely aware of the significant threat posed by the proliferation of inexpensive, expendable drones to traditional air defense systems. Understanding this, each military branch, in partnership with industry, is testing a variety of ways to defeat UAS attacks.[7] There are several C-UAS solutions already in development and production, each with its own benefits and drawbacks. However, the most promising solutions are those that are effective, cost-efficient, and capable of targeting drone swarms. The following are major C-UAS categories available today that utilize different methods to mitigate drones.

Kinetic C-UAS Drones

How does it work?

Like munitions, kinetic C-UAS solutions use physical force to intercept or disable hostile drones. However, this more contemporary approach uses drones specifically designed to collide with, shoot down, or capture hostile UAS.

Examples

- "Kamikaze" drones that collide with and destroy hostile UAS (e.g. Anduril's Anvil and Roadrunner)
- Drones with nets that capture hostile UAS

Benefits

- Hostile drones captured by nets can be analyzed for intelligence such as its origin or maker
- Kamikaze drones are highly mobile and can destroy fast-moving UAS

Drawbacks

- Targets drones individually, thus ineffective against drone swarms
- Kamikaze drones are single-use and therefore more expensive
- Like munitions, there is a heightened risk of collateral damage
- Fast-moving drones can prove difficult to capture

Radio Frequency (RF) Jamming

How does it work?

Jamming solutions emit electromagnetic signals that disrupt a hostile drone's communication. This prevents it from receiving instructions from GPS or its operator and can cause it to lose control or enter a failsafe mode.

Examples

- Directional Jammers
- Omni-Directional Jammers
- Handheld Jammers

Benefits

- Omni-directional jammers can temporarily incapacitate all drones in an immediate area
- Handheld jammers are portable, easy to operate, and relatively inexpensive

Drawbacks

- AI-enabled drones can be programmed to take default action once disconnected from communication or GPS, such as continued navigation toward a target
- Jamming requires strong signal strength, continuous transmission, and proximity to the target
- Jamming may interfere with nearby communications or navigation systems
- The operator may regain control if the jammer stops transmitting or the drone returns to its launch point
- Directional and handheld jammers struggle against drone swarms
- Omni-directional and handheld jammers have a limited range

Spoofing

How does it work?

Spoofing broadcasts a false signal into a drone's receiver, such as GPS, which can alter a drone's perceived location, altitude, or flight path. The drone then responds or acts according to the spoofed information.

Benefits

- The hostile drone can be recovered for intelligence

Drawbacks

- Similar to jamming, spoofing can interfere with nearby navigation systems or friendly UAS
- Does not fully take over a hostile drone
- Requires a more powerful signal than the drone operator's

Cyber Takeover

How does it work?

Cyber takeover solutions transmit radio frequency signals that allow a remote operator to take full control of a hostile drone and land it safely in a predefined zone.

Benefits

- The hostile drone can be recovered for intelligence

Drawbacks

- The system's information library must be continuously updated to counter constantly evolving drone types
- May be less effective if a hostile drone uses non-standard frequencies or optical navigation instead of GPS
- Requires advanced technical expertise
- Requires a more powerful signal than the drone operator's
- Could struggle against drone swarms if each drone operates on different frequencies or protocols

---

High Energy Lasers

How does it work?

This solution employs sustained laser beams to disable or disrupt a drone's components.

Benefits

- Unlimited magazine
- Can be effective at long range

Drawbacks

- Requires sustained targeting to affect a drone's components
- Targets drones individually, thus ineffective against drone swarms
- Highly expensive, 250 kW class and 60 kW class lasers are estimated to cost $200 million and $100 million per unit, respectively[8]
- Ineffective against small, fast drones
- Requires a huge power source
- Bad weather, battlefield obscurants, and other line-of-site factors can render lasers ineffective
- Very high development, production, maintenance, and support costs
- Mean-Time Between Failures (MTBF) is low
- Mean-Time-To-Repair (MTTR) is high
- Lasers have fundamental size, weight, power, and cooling challenges

---

High-Powered Microwave (HPM)

How does it work?

HPM solutions also use directed energy to target a drone's components. Unlike lasers, however, HPM solutions create a cone of electromagnetic interference that disables electronics over both narrow-band and wide-band areas.

How are Modern, Long-Pulse HPM Systems Changing the C-UAS Game?

While older HPM systems were more cumbersome and less accurate, advancements in technology have revolutionized this C-UAS solution. Modern HPM systems use solid-state, gallium nitride (GaN) RF amplifiers, which have greatly improved the solution's size, weight, and power considerations. Equipped with GaN technology, modern HPM systems produce magnitudes more energy than legacy HPM systems which use vacuum tubes for amplification.

The Electronic Warfare Cat and Mouse Game: Hardening against HPM

While some have theorized that hardening drones with copper tape or other commercial off-the-shelf (COTS) materials can render HPM ineffective, a 2021 Office of Naval Research project titled, "Red Team UAS Hardening for Counter HPM" concluded that COTS materials, including copper tape, often made targets more susceptible to HPM and that it takes significant expertise in electromagnetic shielding, drone construction, and drone flight mechanics to effectively shield drones against HPM.

Modern GaN-based HPM Benefits

- Unlimited magazine
- Broad targeting spectrum and high rates of fire are effective against drone swarms
- Requires less power than legacy HPM
- Fires longer pulses and significantly more energy than legacy HPM
- Reduced size makes the system more mobile than legacy HPM
- Can safely operate in close proximity to ordinances, people, and fuel
- Costs pennies per shot compared to costly traditional munitions such as missiles
- Works in all weather conditions

Challenges

- Using wider beams to counter drone swarms reduces effectiveness at longer ranges

The Most Effective C-UAS Solution?

A Layered Defense Approach

Military leaders are advocating for a layered defense approach to optimize defense against the emergent and evolving asymmetric threat of drones. A layered defense approach uses early warning and detection systems alongside both kinetic and non-kinetic countermeasures to provide 360-degree, short-range, medium-range, and long-range air defense. This approach should include effective threat detection radar and an always accessible variety of both soft-kill and hard-kill options, allowing for rapid response to changing threat environments. For example, kinetic C-UAS drones could be used to destroy or capture single hostile targets at long range, dismounted warfighters could be equipped with handheld jamming C-UAS systems, and HPM systems could provide a last layer of short-range defense against group 1-2 drones and drone swarms, saving the more expensive air defense missiles for more strategic targets.

This approach has been echoed by senior leaders at the forefront of this challenge. In a March 2024 Senate Armed Services Committee hearing, Commander of U.S. Central Command Gen. Erik Kurilla expressed a need for a layered defense and one that includes HPM C-UAS systems to counter drone swarms.[9] Ultimately, incorporating multiple layers of diverse C-UAS technologies is the most effective method for countering a myriad of potential threats. Moreover, a layered defense is also advantageous in sensitive areas with civilian populations and a heightened need to minimize collateral damage.

Final Considerations

The era of asymmetric drone warfare has certainly arrived and is here to stay. In light of this, the development of effective C-UAS capabilities—especially against cheap, easily produced drones and drone swarms—must be a persistent priority for the Defense Department moving forward. It is critical that our armed forces stay at the forefront of these technological advancements in order to maintain a decisive advantage on the battlefield, especially against a near-peer adversary.

EPIRUS

A Message from our Sponsor

Warfare is undergoing a revolutionary paradigm shift: from expensive, centralized platforms and units, to distributed formations and attritable systems. Gone are the days when the supply chains needed for ammunition resupply, fuel depots, and thousands of support troops needed to keep an army fighting could only be observed intermittently and out of range from attack. Given the proliferation of drones and other ISR advancements, the entire area of operations is a battlefield with nowhere to hide - leaving expensive platforms and centralized units vulnerable to attack and costly, traditional air defenses at risk of being overwhelmed by large quantities of cheap drones.

Epirus was founded in 2018 with this paradigm shift, and the need to defend against drone threats, in mind. Instead of relying on traditional technologies like traveling-wave tubes and vacuum tubes, we took a novel approach to High-Power Microwave (HPM), leveraging Gallium Nitride (GaN) semiconductors. The result is Leonidas, our solid-state, software-defined, long-pulse HPM systems with an unlimited magazine and unmatched size, weight, and power benefits for counter electronics.

Within Leonidas is an array of Gallium-Nitride-based Line Replaceable Amplifier Modules (LRAMs) that feature unique power management, control, and amplification characteristics. This LRAM architecture enables modularity and scalable design flexibility so we're able to rapidly introduce new form factors to meet the constantly evolving mission needs of our customers.

This is not a future technology. It is a now technology — necessary to shift the cost and strategic balance back in our favor. With more than 100,000 sq. ft. of warehouse space in Torrance, Calif., we are production-ready, today.

At Epirus, we are dedicated to our mission of overcoming the asymmetric challenges inherent to the future of national security. Direct your energy with us and innovate with impact.

Epirus, Inc.

About Forecast International

Forecast International, a GovExec company, has been a premier provider of market intelligence services to the worldwide aerospace, defense, military electronics, and power systems industries for over 50 years. With a focus on long-range forecasting, our proprietary information is trusted by governments and some of the largest organizations in the world. FI's editorial group consists of 15 full-time analysts who have more than 250 years of combined experience with the company. Our expert analysts have served our clients throughout shifting markets and evolving global events. In an ever-evolving landscape, data and intelligence are central in making today's forecast tomorrow's reality.

About Epirus

Epirus is a technology company developing electronic warfare systems with unprecedented counter-electronics effects to protect against emerging threats.

Visit our website to learn more about our innovative approach and cutting-edge product lines.

For more information on Epirus' solutions or to request an interview with subject matter experts, please contact media@epirusinc.com.

Endnotes

1. https://media.defense.gov/2022/Mar/14/2002956269/-1/-1/1/SUAS%20IDENTIFICATION%20AND%20REPORTING%20GUIDE.PDF
2. https://www.twz.com/drone-swarm-launcher-truck-displayed-at-chinas-big-arms-expo
3. https://apnews.com/article/us-china-drone-swarm-development-arms-race-e5808a715415d709f466da00cdeab10f
4. https://breakingdefense.com/2024/05/high-price-of-red-sea-shootdowns-speeds-navys-pursuit-of-cost-effective-solutions/?utm_campaign=BD%20Daily&utm_medium=email&_hsenc=p2ANqtz--UlK8SRJmZ4PMvaS6_-aMGY5qeV4kzv8DCs-5GwCRDR0SeiyU42p-3wqU2hFagZcPPcFp9RmPmiSX7E7Y4P330D4KEINQ&_hsmi=307263024&utm_content=307263024&utm_source=hs_email
5. https://archive.ph/EqJHY
6. https://archive.ph/EqJHY
7. https://www.defense.gov/News/News-Stories/Article/Article/3588869/countering-unmanned-aerial-system-attacks-a-priority/
8. https://sgp.fas.org/crs/weapons/R44175.pdf
9. https://www.centcom.mil/MEDIA/Transcripts/Article/3700887/senate-armed-services-committee-hearing-posture-of-united-states-central-comman/

FORECAST INTERNATIONAL

Address | 75 Glen Road, Ste. 302, Sandy Hook, CT 06482
Telephone | + 1.203.426.0800
Fax | 203.426.0223
Website | forecastinternational.com