The Drone Killers

Warfare in the New Millennium

BY **TOM ATWOOD**

The extreme need for anti-drone defenses was clearly demonstrated in September 2019, when Houthi rebels in Saudi Arabia used relatively inexpensive drones to disable five percent of the world's oil supply in a single attack. For a few thousand dollars and almost no man-power, Third World insurgents inflicted billions of dollars of damages on nations worldwide. A new form of guerilla warfare is upon us.

SHUTTERTOCK

On September 14, in a report titled "Drones Strike Big Saudi Oil Centers, and Houthis Claim Responsibility," it was reported at the NYTimes.com by Ben Hubbard, Palko Karasz, and Stanley Reed that drone strikes had set fire to a Saudi Aramco refinery in Abqaiq, Saudi Arabia, earlier that Saturday. The *New York Times* reporters stated that "Yemen's Houthi rebels launched drone attacks on key Saudi oil facilities on Saturday, setting off blazes that could be seen from space and showcasing how cheap new technologies allow even minor militant groups to inflict serious damage on major powers."

Saudi Aramco, according to Wikipedia, is one of the largest companies in the world. Headquartered in Dharan, Saudi Arabia, it has recently been poised to offer a public IPO, making the attack all the more inopportune. The Houthis claimed to have used 10 drones in the attack. Independent sources have indicated that such drones can be purchased, equipped with munitions, and deployed for a relatively low cost of 10,000 to 15,000 USD each. This illustrates the emerging phenomenon of "asymmetric warfare," in which weaponized drones can be used in swarms by small militant groups at a relatively low cost to strike at nation states possessing far greater military, financial, and technical resources.

U.S. Secretary of State Mike Pompeo was reported in national media to have guaranteed the Saudis the United States' full support to defend against this emerging threat. As this dramatic development unfolds, it begs the question of how anyone can best defend against a swarm drone attack. What defenses are under development or deployed at this time? This is the backstory with a summary of selected C-UAS systems that have appeared at recent annual AUVSI Xponential trade shows.

Only federal agencies, law enforcement, and the military are legally permitted to operate drone-suppression (jamming) equipment. Federal law prohibits the operation, marketing, or sale of any type of jamming equipment, including devices that interfere with cellular and personal communication services (PCS), police radar, global positioning systems (GPS), and wireless networking services (Wi-Fi).

Putting the growing investment in C-UAS (counter-UAV) in perspective, it has been reported that the Pentagon will spend almost twice as much on countering drones in 2019 as it did in 2018.

AS CONCERNS GROW AROUND THE POTENTIAL SECURITY THREATS DRONES MAY POSE TO BOTH CIVILIAN AND MILITARY ENTITIES, A NEW MARKET FOR COUNTER-DRONE TECHNOLOGY IS RAPIDLY EMERGING.

The Bard College Report

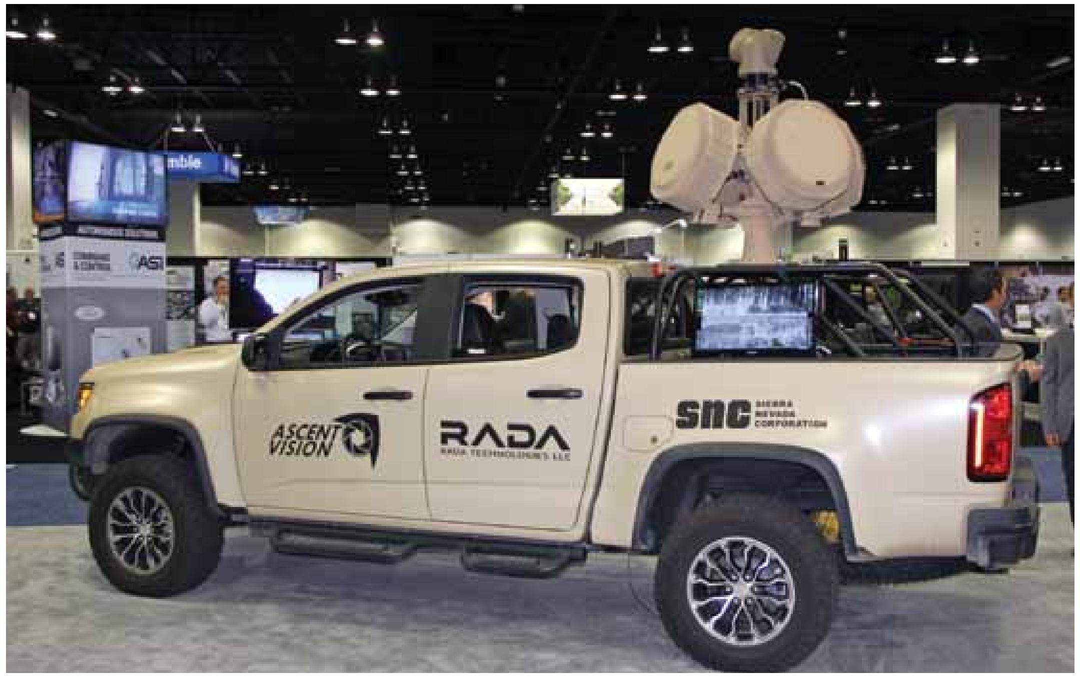
Bard College, located in New York State, published a detailed report in February 2018, titled "Counter-Drone Systems 2018" that assessed the then-status of C-UAS technologies. Bard College has announced that a second, followup report is scheduled for autumn 2019. The 2018 report introduction notes: "Counter-drone technology, also known as counter-UAS, C-UAS, or counter-UAV technology, refers to systems that are used to detect and/or intercept unmanned aircraft. As concerns grow around the potential security threats drones may pose to both civilian and military entities, a new market for counter-drone technology is rapidly emerging. To date, we have found at least 235 counter-drone products either on the market or under active development. This report provides background on the growing demand for C-UAS technology, describes how the technology works, presents our database of known C-UAS systems from around the globe, and explains some of the challenges surrounding counter-drone technology use."

The report notes "Key Takeaways":

- The C-UAS industry has grown exponentially in recent years. We have identified over 230 C-UAS products produced by 155 manufacturers in 33 countries;
- The most popular drone detection techniques are radar, RF detection, EO, and IR. The most popular interdiction technique is jamming;
- C-UAS technology poses a wide range of practical, legal, and policy challenges in all operating environments;
- A lack of common standards in the C-UAS industry means that there is a wide variance in the effectiveness and reliability of systems.

Some of the leaders in C-UAS manufacturing offer a variety of drone defenses that vary widely in terms of technology, portability, complexity and expense.

Ascent Vision's mobile air defense system was exhibited at the 2018 Denver Xponential trade show and conference. Radar, optics, and electronic signal jamming can be deployed by this all-terrain vehicle traveling at 40mph on rough terrain. Note the RF signal emitter atop the off-road-truck's bed.



LUCIEN MILLER/TOM ATWOOD

ASCENT VISION

Ascent Vision, based in Bozeman, Montana, specializes in precision technologies for the unmanned systems industry. Disciplines it specializes in include counter-drone technology, aerial firefighting sensors, airborne ISR, maritime sensors, and lightweight UAV imaging payloads. It manufactures and distributes worldwide topline gimbal systems. It offers a full-package C-UAS system for fixed site and mobile solutions with its X-MADIS eXpeditionary Mobile Air Defense Integrated System. Technologies used include radar, optics, and electronic signal jamming, and these can be deployed by an all-terrain vehicle traveling at 40mph on rough terrain.

DRONE SPEAK TRANSLATED » Counter-Unmanned Systems Terminology Basics

One of the ironies of "unmanned systems" speak is that although remotely piloted vehicles have no human pilots onboard, there are, in fact, typically significantly more humans involved in planning, preparing, controlling, and monitoring unmanned systems flights than is the case when human pilots are onboard an aircraft. Today, there are far more unmanned aerial systems pilots in training and on the job than there are military pilots of manned aircraft that historically performed aerial inspection, surveillance, and recon (ISR).

C-UAS drone technology has become quite sophisticated and often uses combined sensor arrays to increase the likelihood of detecting intruders. For example, a radar sensor may trigger acoustic and optical sensors. The following terms and abbreviations are frequently used.

AGL Above ground level

AI Artificial Intelligence, or AI for short, refers to the ability of a digital robotic computer to perform a set of tasks commonly performed by humans.

Combined Interdiction Simultaneous GNSS and RF jamming.

Electro-Optical (EO) Sensing Drone detection based on visual signature

GNSS Global Navigation Satellite System, which refers to automated geo-spatial positioning data for GPS, GLONASS, Galileo, Beidou and similar geo-location systems.

Infrared (IR) Sensing Drone detection based on heat signature.

JammingThe disruption of GNSS data flow to drones.

Machine Learning An application of AI that enables computer systems to autonomously learn without additional human programming.

MRO Drone maintenance, repair, and operations.

Spoofing Controlling a targeted drone by compromising its communications link.

RF Radio Frequency.

ROV Remotely operated vehicle.

TCL Technical Capability Level, a term of art used by NASA and federal agencies to designate drone authorization permissions; for example, to fly over populated areas in urban areas.

UAV-based Interdiction Drone-mounted counter measures for close-in airborne disruption.

UTC Coordinated Universal Time, used for synching drone operations.

UAM Urban Air Mobility, refers generally to safe air traffic operations in an urban area for both manned and unmanned systems.

UTM Unmanned Systems Traffic Management.

DRONESHIELD

Among the most authoritative sources supporting the C-UAS market is DroneShield. Based in Sydney, Australia; Virginia; Washington, DC; and London, DroneShield is a worldwide leader in drone security technology. The company has developed preeminent drone security solutions that protect people, organisations, and critical infrastructure from intrusion from drones. Its leadership brings world-class expertise in engineering and physics, combined with deep experience in defence, intelligence, and aerospace. DroneShield provides effective countermeasures to drone intrusions to help public and private sector customers take proactive measures against airborne threats to safety, security, and privacy.

DroneShield has defined the drone market by dividing it into categories. These distinguish UAS by weight, operating altitude, and speed. It also defines threat categories with three elements: nuisance, gathering of intel, and delivering contraband or explosives. DroneShield offers a free Counterdrone Handbook on its website, published August 2019. Their products use sophisticated electronics including a multisensor detection system incorporating radar systems and cameras, and these sensor systems are combined with a jammer to defeat UAS.

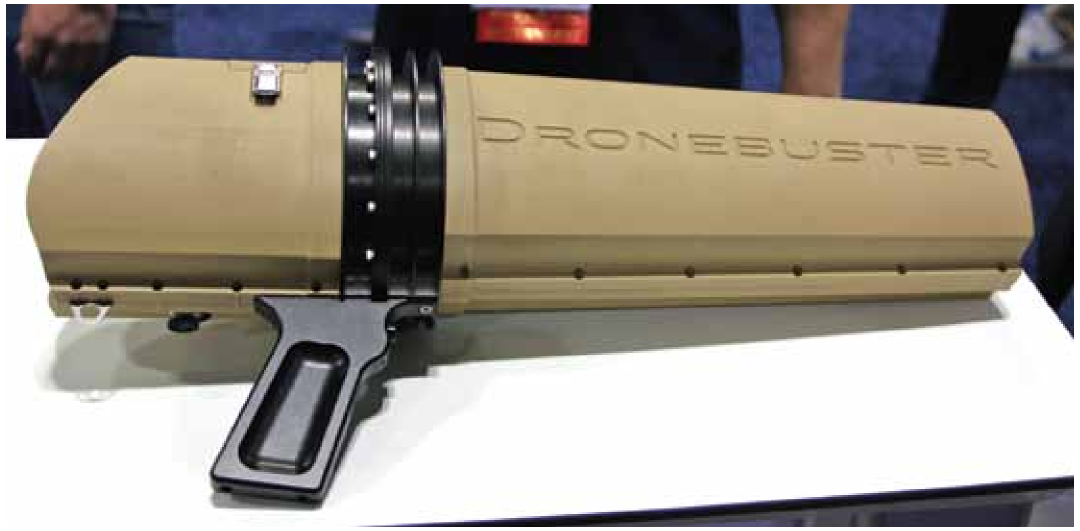
DroneShield technology distinguishes UAS by weight, operating altitude, and speed, and further assesses mission intent, whether nuisance, intel, or delivery of contraband or explosives. A multisensor detection system, incorporating radar systems and cameras, combine with a jammer to defeat UAS.

CITADEL DEFENSE

On May 2, 2019, Citadel Defense received a U.S. Government award to expand development of their C-UAS technology. Lt. Col. (R) Matt England, U.S. Army, and now vice president of Business Development for Citadel, is quoted on the company's website: "Our Titan CUAS system autonomously clears the Warfighter's airspace, allowing them to be unconcerned with threat drones and purely focused on the mission at hand..." The Citadel Defense Titan system, which is depicted as a virtual protective dome, detects approaching drones and classifies whether there is a single unit or a swarm, and reports this in real time to its operators, which can be military, governmental, or commercial users. The system uses sophisticated electronic countermeasures to induce the drone to land or return to its home base. Enabling technologies include a mix of machine learning algorithms, artificial intelligence, and "software-defined hardware technology" that rapidly identify airborne intruders before they pose a threat.

The Citadel Defense Titan system, which is depicted in this artist's rendition as a virtual protective dome with drones hovering outside its confines, detects approaching drones and reports this in real time to its operators. The system uses sophisticated electronic countermeasures to induce the drone to land or return to its home base. Machine learning algorithms, artificial intelligence, and "software-defined hardware technology" rapidly identify airborne intruders.

ILLUSTRATION BY CITADEL DEFENSE



LUCIEN MILLER/TOM ATWOOD

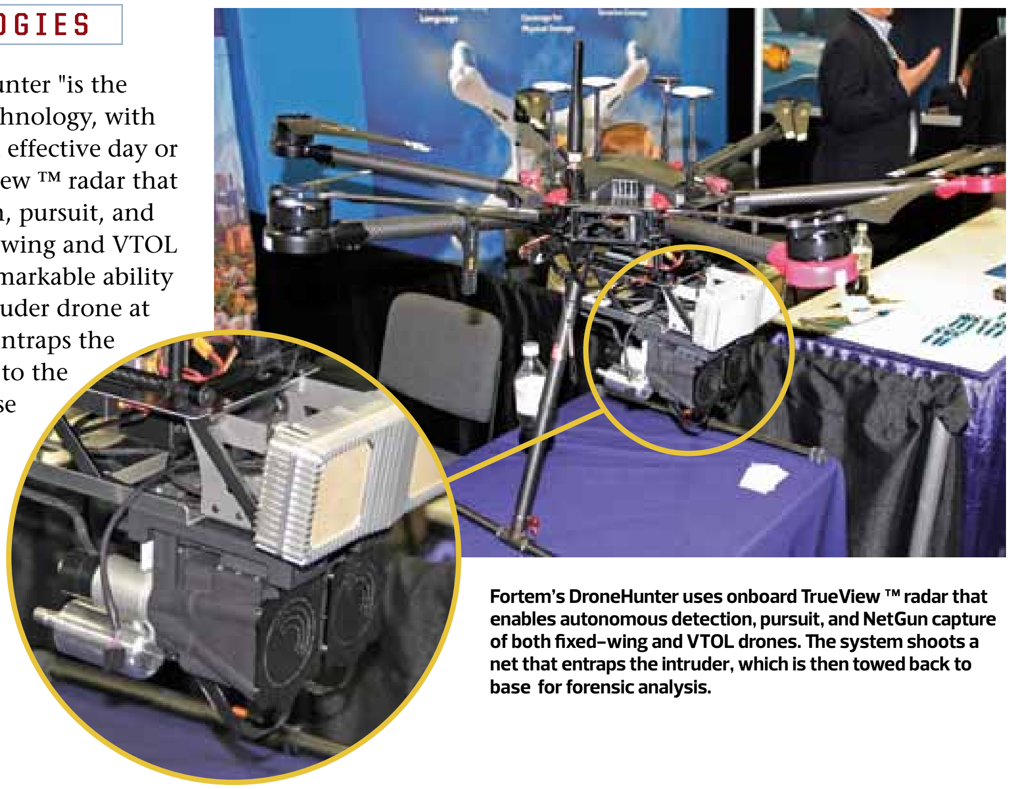
This hand-held electronic gun permits the operator to intercept an intruding drone's command link and command the drone to land or return to its home base. The system achieves this by exploiting weaknesses in COTS 915 MHz, 2.45 GHz, 5.8 GHZ, and HAM radio communication protocols. It also identifies messages sent by the intruder as video, telemetry, or other, and can optionally be equipped with GPS disruption capabilities.

DRONEBUSTER

The "Dronebuster" is among several tools fielded by the U.S. Army to counter unmanned aerial systems. Weighing only five pounds, it is designed for soldiers at remote locations or on dismounted patrols. Dronebuster's onboard electronic tools enable a security team to identify and deal with an approaching unmanned aerial system. These tools permit the operator to intercept the drone command link and command the drone to land or return to its home base. The system achieves this by exploiting weaknesses in COTS 915 MHz, 2.45 GHz, and 5.8 GHZ communication protocols. It similarly exploits weaknesses in HAM radio 433, 445, and 455 MHz communication protocols to force a landing or return to home. The system also enables operators to identify messages sent by the intruder as video, telemetry, or other. The unit can optionally be equipped with GPS disruption capability for jamming GPSL1 and GLONASS L1 frequencies. It is designed for easy updating as new drone technologies emerge.

FORTEM TECHNOLOGIES

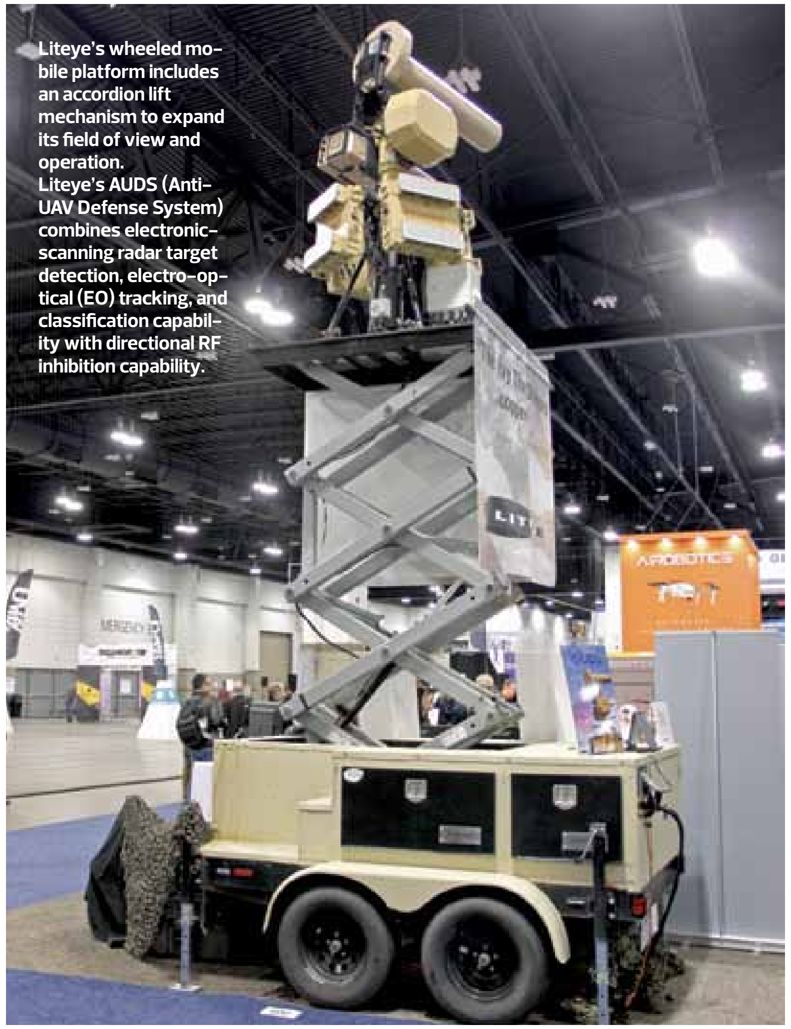
Fortem notes that its DroneHunter "is the ultimate drone-interceptor technology, with over 3,500 real-world kills and effective day or night." It uses onboard TrueView ™ radar that enables autonomous detection, pursuit, and NetGun capture of both fixed-wing and VTOL drones. The system has the remarkable ability to physically approach an intruder drone at altitude and shoot a net that entraps the intruder, which is then towed to the DroneHunter's operational base for later forensic analysis.



LUCIEN MILLER/TOM ATWOOD

Fortem's DroneHunter uses onboard TrueView ™ radar that enables autonomous detection, pursuit, and NetGun capture of both fixed-wing and VTOL drones. The system shoots a net that entraps the intruder, which is then towed back to base for forensic analysis.

LITEYE SYSTEMS, INC.



LUCIEN MILLER/TOM ATWOOD

Liteye's wheeled mobile platform includes an accordion lift mechanism to expand its field of view and operation.
Liteye's AUDS (Anti-UAV Defense System) combines electronic-scanning radar target detection, electro-optical (EO) tracking, and classification capability with directional RF inhibition capability.

Liteye Systems, Inc. is a leading provider of rugged, high-resolution, helmet-mounted displays (HMD), micro-imaging viewfinders, and thermal and radar surveillance systems. The company notes that: "Liteye's AUDS (Anti-UAV Defense System) is a counter-drone defense system that is designed to disrupt and neutralize unmanned aerial vehicles (UAVs), or unmanned aircraft systems (UAS) engaged in hostile airborne surveillance and potentially malicious activity. AUDS is currently deployed with U.S. forces and has numerous confirmed defeats, or kills, of enemy UAS in theatre."

Liteye's counter-unmanned aircraft systems defense technology ("CAUS") combines electronic-scanning radar target detection, electro-optical (EO) tracking, and classification capability with directional RF inhibition capability. CUAS is a smart-sensor and effector package capable of remotely detecting small UAS and then tracking and classifying one or more intruders before providing the option to disrupt their activity. The company notes its anti-drone products may be used in remote or urban areas to prevent UAS being used for terrorist attacks, espionage, or other malicious activities against sites with critical infrastructure. CUAS can also serve as a ground surveillance system. Liteye integrates systems and trains operators out of their Colorado facility.

INVISIBLE INTERDICTION, INC.

Invisible Interdiction, a Florida-based company, was founded in the spring of 2018. The company reports that it offers the lowest-power, highest-performing C-UAS system on the market. The company specializes in man-portable hand-held systems with full-spectrum electronic jamming capability using known and emerging radio frequency bands. Note that the company represents them to be the smallest and lightest of such systems on the market. Products include hand-held frequency jammers and systems integratable into UAS-detection suites using serial, digital, and Pelco-D interfaces. Recently awarded a Phase III production contract by the U.S. Air Force, the management team has over five decades of combined experience in the U.S. military.

LUCIEN MILLER/TOM ATWOOD

Invisible Interdiction, a Florida-based company, reports that it offers the lowest-power, highest-performing C-UAS system on the market. Products include hand-held frequency jammers and systems integratable into UAS detection suites using serial, digital, and Pelco-D interfaces. It was recently awarded a Phase III production contract by the U.S. Airforce.

We're at the Beginning

It now appears that for every company that is actively designing and building armed drones, there are multiple companies coming up with ever more effective means of rendering them useless. The drone race is only just now beginning and the "swarm" approach, which utilizes large numbers of smaller, less-expensive autonomous units is much more difficult to defend against. Once the target coordinates are input, all a field operator needs to do is crawl within range of the target and press a button, and then stand back and watch them wreak havoc. The face of combat is changing. ✈