D-FEND SOLUTIONS

The Evolving Drone Threat Demands Counter-UAS Tech that Evolves with it:

The Case for a Next Generation, New Technology Category C-UAS

TECH CONSULTING
PEOPLE · PLATFORMS · POLICY

By **Dawn Zoldi** (Colonel, USAF Ret.)
UAS and C-UAS Author, Speaker, Expert

Dawn Zoldi

Dawn M.K. Zoldi, (Colonel, USAF, Retired), is a leading UAS and C-UAS industry speaker and author, licensed attorney with 28 years of combined active-duty military and federal civil service to the U.S. Air Force, founder and Chief Executive Officer of P3 Tech Consulting, and internationally recognized expert on emerging UAS, C-UAS, and air mobility technology, law, and policy. Dawn contributes to many magazines with articles on UAS and C-UAS and hosts popular tech podcasts on the topic.

Dawn has been awarded MOVE America (Mobility) - The Disruptors (2022), Airwards People's Choice - Industry Impactor (2022), eVTOL Insights Powerbook (2022), Top 100 Women in Aerospace and Aviation to Follow on LinkedIn (2022, 2021) and the Woman to Watch in UAS - Leadership Award (2019).

She has strategic partnerships with and leadership roles in multiple aerospace, drone education, non-profit, and media-related companies and organizations. Dawn is a former adjunct professor of homeland security, graduate-level adjunct for UAS law and policy and author of Unmanned Aircraft Systems Legal and Business Considerations: A Modern Primer for U.S. Commercial Drone Programs.

As drones continue to proliferate globally, so too do drone incidents and attacks. Drone intrusions into stadiums and other mass gatherings, illegal drone operations around airplanes, helicopters and airports, border incursions, critical infrastructure and prison contraband-delivery incidents rank high among the increasingly common negative drone encounters in civil society. On the battlefield, adapted small commercial drones have become a mainstay to gather intelligence and deliver both kinetic and non-kinetic payloads. Staying one step ahead of this wide range of threats requires counter-drone technology that evolves with it.

Economics and Accessibility Drive Evolving Threats

In the past, only countries with a lot of money and professional armies could afford to have air power. However, in the 1990s, large drones equipped with weapons and surveillance capabilities, like the Predator, started to be used in battles. These drones quickly became essential for military forces. However, the control of drones by only a few countries did not last long. Small, affordable, and flexible commercial drones became widely available, making air power accessible to almost anyone.

Cheap commercial off-the-shelf (COTS) drones have several characteristics that make them valuable in warfare. Their ability to fly over barriers allows them to access areas that may be difficult or dangerous for ground troops to reach. They can scout out the location of enemy assets and operations, providing valuable intelligence without risking human lives. They can remotely and precisely deliver both lethal and non-lethal payloads to cause significant damage to mission-critical capabilities and opposition forces. The affordability and availability of these drones make them accessible to a wide range of users, from conventional military forces to state and non-state actors, including proxy militant groups. This increases their potential impact on the battlefield.

This cost-effectiveness and widespread accessibility of these drones make them attainable for such a broad spectrum of users, including those who would choose to create mayhem or inflict damage or harm domestically. Drones pose a variety of safety, operational, and security threats in the United States and globally. Below I highlight a few of these areas of concern.

Surveillance and Espionage

Drones can be used for spying on sensitive government or industrial facilities, capturing valuable information that could be used by adversaries. Drones can be used by hostile foreign intelligence agencies and criminals to collect intelligence (e.g., document activity patterns or the physical layout of targeted facilities), enable espionage, steal sensitive technology and intellectual property, and conduct cyber-attacks against wireless devices or networks. Equipped with a variety of payloads such as cameras, sensors, smartphones, Raspberry Pi or Wi-Fi Pineapple devices, drones can spy on people, facilities and even hack into all kinds of systems, networks, and databases.

In February 2023, St. Charles Parish, Louisiana sheriffs arrested two men from New York for flying a drone over three chemical plants, Dow Chemical, Linde, and American Air Liquide. Also in Louisiana, a year before that, local authorities observed drones flying over chemical facilities and a pipeline. In fact, from 2021-2022, the FBI identified 235 reports of suspicious drone flights at or near chemical plants in Louisiana. Similar Unmanned Aircraft Systems (UAS) incidents also occurred at oil storage facilities in Oklahoma and natural gas facilities in Texas.

Critical infrastructure owners and operators are not the only enterprises at risk for drone surveillance and espionage. In 2017, Apple declared its campus a "no drone zone" and reportedly hired a specialized security force to help it stop drones from flying over its buildings. Other corporations including Meta (formerly Facebook) and Tesla also have reported incidents of drone espionage attempts.

Physical Attacks

Weaponized drones can carry out attacks on civilian and military targets. Over the past few years, militant groups worldwide have regularly used small commercial drones for attacks. For example, in 2019, a small drone armed with explosives killed six military officers in Yemen when it detonated above them. Both Russian and Ukrainian forces have adopted similar strategies and methods. Both sides have used drones designed to hover over a target before detonating, including kamikaze drones that are intended to be destroyed in an attack and drones carrying improvised explosive devices.

Beyond the battlefield, drones have been used in a civil context to conduct physical attacks, including political assassinations. In 2018, two drones detonated in Venezuela over the country's president, who was giving an outdoor speech, in a failed assassination attempt.

Air Traffic Disruption

Drones flying near airports or in restricted airspace can disrupt commercial flights and pose a danger to crewed aircraft. Just this summer, Pittsburgh International Airport suspended operations for approximately 30 minutes due to reports of an unauthorized drone sighting on the northern section of the airfield.

The Federal Aviation Administration (FAA) website notes, "Reports of unmanned aircraft (UAS) sightings from pilots, citizens and law enforcement have increased dramatically over the past two years. The FAA now receives more than 100 such reports each month." Its most recent Reported UAS Sightings report, from January to March 2023, documented over 300 drone sightings.

Smuggling & Cross Border Incursions

Drones can be used to transport illegal goods, such as drugs or contraband, across borders or into secure areas. According to the Testimony of Samantha Vinograd, Assistant Secretary (Acting) for Counterterrorism, Threat Prevention, & Law Enforcement, Office of Strategy, Policy, and Plans at Department of Homeland Security to Congress, from August 2021 to May 2022, U.S. Customs and Border Protection (CBP) detected more than 8,000 illegal cross-border drone flights at the southern border, averaging nearly 900 incursions per month.

Since 2019, Vinograd noted, CBP officers have seized hundreds of pounds of methamphetamine, fentanyl, and other hard narcotics that drug traffickers attempted to transport through thousands of cross-border drone flights. CBP assesses that Transnational Criminal Organizations (TCOs) are pursuing the use of larger drones with increased speed, range, and payload capacity to fly faster, higher, farther, and with more contraband in an effort to evade CBP and law enforcement.

Property Damage

Besides attacks on people, drones can cause property damage, either accidentally (e.g., by crashing into buildings) or intentionally (e.g., by carrying a payload designed to cause damage). In 2020, a modified drone was used to target energy infrastructure in Pennsylvania. It appeared the drone operator intended to damage or disrupt the electric equipment at a power substation in this first reported attack on critical infrastructure in the U.S.

Worldwide drone incidents reported by media in the public domain are tracked and posted on The Global Drone Attack & Incident Tracker, found on D-Fend Solutions' website.
(https://d-fendsolutions.com/drone-incident-tracker/)

Next Gen Detection and Mitigation – A New C-UAS Technology Category

The widespread availability and affordability of drones, and general difficulty in detecting them, and the potential secondary effects of employing mitigation technologies, make drones a challenging threat to manage.

However, in a relatively recent technological development, one of the most accurate and precise ways to take out rogue drones has emerged, namely radio frequency (RF) cyber-based counter drone detection and takeover mitigation systems, which continue evolving with the threat to provide a safe and reliable solution for the military, law enforcement and critical infrastructure owner/operators.

D-Fend Solutions' EnforceAir2 RF Cyber Technology

D-Fend Solutions, creators of proven cyber radio frequency (RF) detection and takeover mitigation technology, has just honed and adapted its premier EnforceAir solution to further meet these needs and now provides even more operational flexibility, higher performance, and more power, in a compact form factor: EnforceAir 2.

D-Fend Solutions' technology works by quietly scanning the radio frequency (RF) environment in a large area. It uses advanced RF cyber detection to spot and identify drones nearby. This avoids false alarms and lets the system tell the difference between a drone and other objects, such as birds or even authorized drones, even when there are lots of other RF signals around.

The system can find, determine, and understand the unique communication details of a drone, like make, model, and serial number, and check these against a large and constantly updated knowledgebase of communication protocols, including for commercial drones that have been altered or tampered with.

EnforceAir can find where a drone took off from and help locate the pilot. The same technology that identifies and determines a drone's unique communication details can also find its takeoff location with accuracy in real time, without needing a clear line of sight. This often leads straight to the location of the pilot flying the drone or a search area around their recent location.

With EnforceAir's active cyber solution, the pilot loses access to control of the drone's communication. This gives EnforceAir system operators, either manually or autonomously, the power to decide how to handle rogue drone incidents. Unlike other systems that can affect RF signals or other communications and cause other unintended harm, D-Fend's EnforceAir system has a special RF cyber takeover mitigation technology that can automatically take control of a rogue drone and gives the system operator the option to either fend it off, that is push the drone away, or take control of it to fly it along a predetermined route to a safe landing. The system does all this very precisely, safely, and without causing any interference or disruption.

EnforceAir comes in several configurations: tactical, military and covert vehicle, stationary and semi-stationary pole mount, man-portable, and stand-alone core unit. Users covering larger protected areas can manage all these modalities through the company's Multi-Sensor Command & Control system (MSC2). MSC2 allows users to manage multiple different EnforceAir deployment kits simultaneously and remotely from a single server.

Just as the drone threat continues to evolve, so does EnforceAir, as reflected here in D-Fend's recent introduction of the EnforceAir2 upgraded version.

EnforceAir2 – More Power and Portability

The new EnforceAir 2 (EA2) brings enhanced cyber detection and takeover mitigation capabilities in a smaller and more portable package, with even greater range and more power.

EA2 comes in all the same modalities as the original EnforceAir, now with even more flexible bundles, and can be fully integrated with the MSC2, with improved SWaP. EA2 also includes a brand-new compact man-portable backpack deployment version. The EA2 backpack deployment option, ideal for covert operations or rapidly deployable counter-drone capabilities on-the-move, provides full counter-drone functionality.

EA2 accommodates a wide range of tactical and operational scenarios, conditions, and terrains, and includes multiple input multiple output (MIMO) 360-degree omnidirectional antennas that can be covertly concealed, and composite and weather-resistant fabric for the backpack.

The rugged, slim, and lightweight EA2 core unit itself can operate in extreme temperatures from -30°C (- 22° F) to +50°C (122° F). The batteries provide 2.5 hours of continuous coverage and can be easily hot swapped in the field. That coverage is long range and compliant, typically detecting threats as far away as 4.5km (2.7 mi) detection range with mitigation range typically from 1.2km (.75 mi) to 4km (2.5 mi), but with instances of much longer ranges common, using approved MIL STD 810H, MIL STD 461 and IP66 frequencies. It also incorporates real-time edge processing.

Regardless of configuration, EA2 also comes with quick setup locking and release mechanisms that enable rapid conversions during changing operational situations.

All these capabilities, in a compact, lightweight, and ready-to-move package maximize combat and security effectiveness.

Unparalleled Situational Awareness and Operational Continuity

As the drone threat continues to change and grow, so does EnforceAir. With unparalleled situational awareness and operational continuity with safety-by-design, EA2 is a major advancement in C-UAS to overcome counter-drone tech deployment challenges. It puts unprecedented power, flexibility, and portability in the hands of protectors and defenders to confront and overcome the growing risks and challenges of ever-evolving drone dangers.

To learn more about EA2, visit
https://d-fendsolutions.com/enforceair2-next-gen-c-uas/

See Yaniv Benbenisti discuss EA2 with Dawn Zoldi in the EA2 World Premiere
https://www.youtube.com/watch?v=VUqLhXcmuag