TESTIMONY OF

Carl Landrum
Vice President of Civilian Programs and Strategy
Dedrone

BEFORE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Border Security and Enforcement
Subcommittee on Oversight, Investigations, and Accountability

Hearing Entitled: "Smart Investments: Technology's Role in a Multi-Layered Border Security Strategy"

ON

July 9, 2024
Washington, DC

Dedrone
45662 Terminal Dr., Suite 110
Sterling, VA 20166
USA
+1 703 2608051

INTRODUCTION

Chairmen Higgins and Bishop, Ranking Members Correa and Ivey, and distinguished Members of the Subcommittees, thank you for the opportunity to testify before you today on behalf of Dedrone. I hope that my testimony will help the Subcommittees better understand the emerging threats in the airspace along our international borders and that sophisticated technological solutions exist to counter these threats.

My name is Carl Landrum and I am the Vice President of Civilian Programs & Strategy at Dedrone. Dedrone is a U.S.-based global provider of state-of-the-art airspace security solutions with the mission to protect people and property from malicious drones, while leveraging technology to allow good drones to fly. Prior to joining Dedrone last year, I had the honor and privilege to serve as a law enforcement professional and senior leader in the Department of Homeland Security (DHS) for nearly three decades. I began my career in 1996 as a Border Patrol Agent in San Diego, CA. After the tragic events on September 11th, 2001, I transferred to become a Federal Air Marshal from 2003 to 2005, and then transitioned back to the Border Patrol. Over the course of my 27 years with DHS, I had the opportunity to work in various roles in multiple sectors along our nation's international borders, including as the Deputy Chief Patrol Agent of the Yuma Sector in Arizona and as the Chief Patrol Agent of the Laredo Sector in Texas.

Beginning in 2015, while I was serving as the Deputy Chief in Yuma, I personally witnessed the genesis of the use of drones by trans-national criminal organizations (TCOs) – also known as cartels – operating on both sides of our international border with Mexico. In those early years, the cartels conducted simple trafficking operations using drones. For example, we observed and recovered drones flying short distances from Mexico into the U.S. carrying small amounts of methamphetamine and black tar heroin. Oftentimes these drones would crash land in backyards demonstrating the initial lack of knowledge, skills and capabilities. At that time, the Border Patrol had no technology-based drone detection capability whatsoever.

From 2015 until my retirement in 2023, and to include my present work in industry supporting U.S. Government customers, I have experienced firsthand the tremendous evolution of the usage of drones by TCOs to further their illicit and deadly activities. While over the same period of time, the U.S. Government's counter-drone technology and capability has lagged far behind. To close this growing capability gap, Congress must ensure that U.S. Customs and Border Protection (CBP) has sufficient resources to leverage commercially available technology and capabilities that can counter TCO drone operations. This investment must be significant, and it must happen now, as nefarious actors around the world are rapidly developing and advancing their drone operations and exporting them to our borders.

FROM EASTERN HEMISPHERE TO WESTERN HEMISPHERE

Since the early days of the ongoing conflict in Ukraine, Dedrone's counter unmanned-aerial systems (C-UAS) have been deployed on the ground along the front line in what has grown into a full-scale drone war between Russia and Ukraine. The tactics, techniques and procedures

(TTPs) used by both countries have rapidly evolved at the 'speed of war' over the past two years and observing these TTPs firsthand continues to provide us with incredibly unique and informative insights and lessons into present and future drone warfare. At the beginning of the war, 'advanced' radio frequency (RF) detection, also known as RF decoding, similar to what is still used on the U.S. borders today, was the primary capability used to detect Russian drone operations and attacks. Today that methodology of drone detection is wholly insufficient and no longer the case in Ukraine. Russia's ability to manipulate and conceal the RF signatures emanating from its drones, through TTPs such as spoofing or cloning, or even fly autonomous drones, means that relying on RF decoding alone for drone detection and location is quickly becoming unreliable and obsolete.

RF decoding reads the RF signal communications between the drone and its remote control to extract data such as GPS coordinates (if available), altitude, and speed. However, there are many limitations to relying solely on decoding as part of a C-UAS apparatus.

- **Encryption:** Many drones encrypt their RF signals to avoid being located. These encryption keys can be easily updated and changed to ensure that decoding remains not only expensive but also unreliable. The moment it is known that an RF signal is understandable, the manufacturer or user can simply leverage a new encryption mechanism.

- **No Location Offered:** Not all drones come equipped with GPS microchips installed. Therefore, if there is no GPS board then there is no coordinate data to extract even if decoding is possible. This non-existent GPS board issue is particularly true when it comes to homemade drones.

- **Spoofing:** Unencrypted drone data can be susceptible to tampering. The concern lies in the potential manipulation of data transmitted by drones, a tactic known as spoofing. Spoofers can alter drone signals, making them appear to originate from a different location or masquerade as another drone altogether. Additionally, spoofers can easily generate a drone signal where there is no drone at all. This presents a substantial hurdle in drone detection efforts, especially when solely relying on RF decoding techniques.

- **Autonomous:** Some drones can be pre-programmed to fly a specific route ahead of launch. With these drones there is no RF signal to direct the drone during flight and thus no RF signal to detect / decode.

Presently, Dedrone observes all these TTPs being implemented on both sides of the conflict in Ukraine to hide the true location of drones. As these TTPs become perfected on the battlefield, it was only a matter of time before these TTPs permeated from the frontline in Ukraine into the Western Hemisphere and along our southwest border. The TCOs operating along and south of our border with Mexico generate tens of billions of dollars each year in revenue from their illicit activities. With this endless supply of funds at their disposal, the cartels invest significant

resources into the latest and most sophisticated drone-related TTPs that will further their illicit activities and generate more profit.

Rooted in long-standing ties between Russia and certain countries in South America, we are beginning to see some of these same TTPs arriving in the Western Hemisphere and making their way to our own U.S. borders. According to open-source media reporting, in October of last year, eight Colombians were arrested in Jalisco, Mexico for constructing improvised explosive devices to be used as payloads on drones for a local criminal gang involved in narcotics trafficking.[1]

I have personally observed the steady maturation of the TCOs' drone operations and use of technology on both sides of the U.S.-Mexico border to thwart CBP's very limited drone detection capabilities.[2] Even out-going Mexican President López-Obrador over the past year has openly called for greater international assistance to help Mexico with its drone problem.[3]

U.S. BORDERS LACK AIRSPACE SECURITY

At present along our international borders, the Border Patrol maintains only basic C-UAS capability, using only decoding RF methodology to detect, track and identify (DTI), from only a single manufacturer, DJI. For context, Dedrone maintains a library of over 150 unique drone manufacturers, from our deployments around the world. Additionally, even with just this basic DTI capability deployed along our international borders, there have been approximately 37,423 flights detected near the border *(within 400 meters)* in FY2024 year-to-date (YTD), of which >2,492 of those drones flew illegally across the border.

Along our southwest border specifically, the use of drones by the TCOs is growing at a rapid rate as they innovate to further their illicit activities. Drones are currently being used by TCOs and other illicit bad actors to:

- Conduct surveillance of U.S. government personnel and facilities along the international border;
- Conduct counter-surveillance on rival TCO and Government of Mexico (GoM) Military positions;
- Provide overwatch and guide groups of migrants attempting to avoid apprehension;
- Provide overwatch and guide individuals and groups smuggling narcotics into the U.S.;
- Physically drop narcotics via drone delivery across the border;
- Physically drop bundles of currency as payments to individuals on the U.S. side of the border.

---

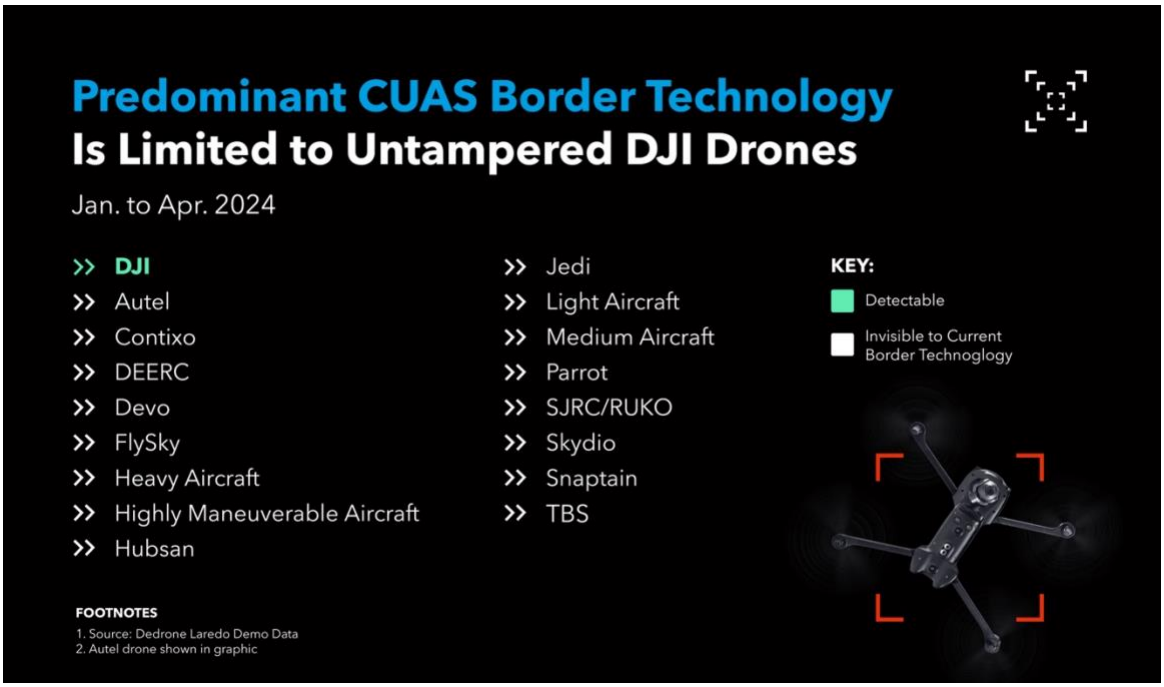
[1] Narcosis, *8 Arrested in Mexico For Manufacturing Drone Explosives*, ATLAS NEWS (Oct. 9, 2023).
[2] *CJNG attack against indigenous community of Michoacán denounced*, EJECENTRAL (Jul. 4, 2024).
Mark Stevenson, *Mexican cartels now use IEDs as well as bomb-dropping drones*, ASSOCIATED PRESS (Feb. 4, 2022).
Gabriel Mondragon Toledo, *NarcoDrones Have Become a Growing Scare Tactic in Mexico's Drug Wars*, INKSTICK (Nov. 7, 2023).
[3] Julian Resendiz, *AMLO seeks enhanced penalties to curtail drone attacks*, NEWSNATION (Aug. 10, 2023).

At the same time TCOs are using drones more frequently, they are also continuously altering their technologies and methods, and flying many different types of drones to defeat USBP's very limited DTI capability – specific to only non-tampered DJI drones. At present, Border Patrol Agents have virtually zero capability to detect non-DJI, modified DJI or encrypted DJI drones.

LAREDO DEMO

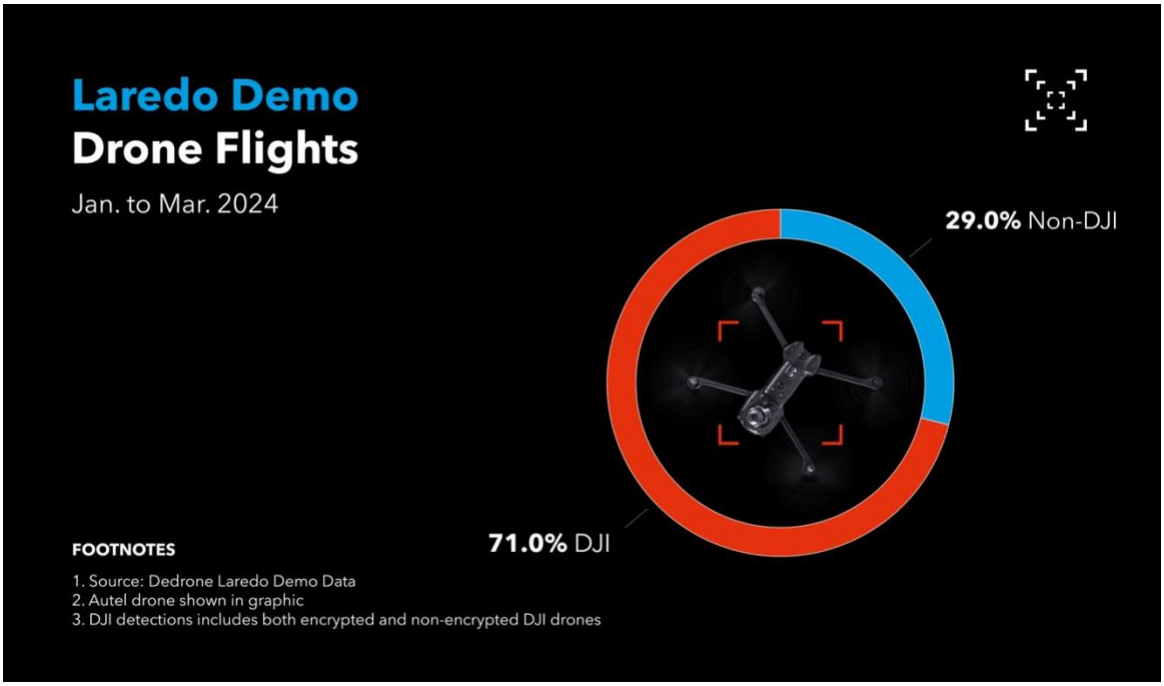
In January of this year, Dedrone entered into an official contract with CBP – at no cost to the government – to perform a demonstration project of C-UAS capabilities along a five-mile stretch of the U.S.-Mexico border in Laredo, TX. To date, Dedrone has invested over $3.3 million to establish full spectrum C-UAS DTI capabilities including RF, radar, and camera sensor hardware, as well as software powered by artificial intelligence (AI), including machine learning and computer vision. This Laredo Demo can detect nearly 600 different drone models including altered drones and even homemade drones.

In addition to non-tampered DJI drones, the Laredo Demo project also detected the following drone types:



In the first 80 days of the Laredo Demo, Dedrone detected 682 unique serial numbers operating along this five-mile section of the border. It is important to note that this accounted for only 71% of the total drone detections made during this period. There were an additional 16 drone manufacturer types that would NOT have been detected but for the Laredo Demo project. These detections comprise 29% of the total made during this period and would not have been detected prior to the Laredo Demo. The full spectrum of sensing capability – RF, radar, and camera –

combined with the AI-driven sensor fusion, temporarily deployed by Dedrone, allow CBP to have complete air domain awareness along these five miles of border. Without it, CBP is limited to their basic DTI capability – specific to only non-tampered DJI drones – and would be blind to 29% of all drone flights.



RECOMMENDATIONS FOR CONGRESS

- **C-UAS Authorization Legislation**
  - We strongly urge Congress to enact comprehensive C-UAS authorization legislation this year to ensure that CBP's C-UAS authorities to protect people and property continue well into the future.
  - We applaud Chairman Green and Ranking Member Thompson for their leadership and tireless work on H.R. 8610, the Counter-UAS Authority Security, Safety, and Reauthorization Act, and we strongly support the framework and principles of the bill.
  - Any authorization must include a multi-year renewal of federal authorities.
    - As is envisioned in H.R. 8610, Congress should enact a multi-year extension and enhancement of C-UAS authorities under 6 USC 124n for federal government agencies like CBP.
    - Providing agencies with adequate certainty over multiple years will allow for better planning and budgeting for C-UAS programs and activities.

- H.R. 8610 also contains provisions that clarify the rules for how and when law enforcement can utilize RF decoding to DTI unauthorized drones. While RF decoding has its limitations, it remains a useful tool, and it is vitally important to clarify the policies law enforcement must adhere to.

- **DHS Appropriations**
  - Increase funding for the procurement of C-UAS capabilities by CBP
    - As the Subcommittees know, the House recently passed a DHS Appropriations bill for FY2025 that included a generous increase in funding to enable CBP to procure additional C-UAS capabilities. Thank you for this very timely and important investment in our border security.
    - Based on my three decades of experience executing and leading border security operations, including the past nine focused on C-UAS threats and capabilities, it is my view that CBP requires a $1 billion program of record to counter current and emerging threats, and achieve appropriate airspace security along our international borders.
    - Based on this metric, I believe that Congress should appropriate $250 million as an initial down payment for the procurement of CBP C-UAS capabilities.
  - Congress should direct and encourage CBP to fund C-UAS programs and activities that move beyond single manufacturer RF decoding including:
    - Expand RF sensing to DTI all RF based drones including spoofed or encrypted drones as well as homemade drones. As previously described, there are many limitations to relying solely on decoding as part of a C-UAS apparatus.
      - Full RF sensing includes localization through different types of triangulation (ie: angle of arrival and time difference of arrival) to offer a more failsafe way to detect and locate drones.
        - Angle of arrival (AOA): Using this method, one sensor can be used to determine the direction of the drone and multiple sensors can be leveraged to calculate the exact position of the drone based on triangulation from multiple direction sensing sensors.
        - Time difference of arrival (TDOA): This method measures the difference in time of arrival between several sensors. TDOA depends on the distance between the drone and sensors.
    - Further enhance DTI capabilities to detect autonomous drones (no RF signal) and drones at greater distances by bringing long-range radar and long-range camera (for visual confirmation and payload detection) into a single fused instance from these multiple sensor types
    - Enhance non-kinetic mitigation capabilities to allow CBP personnel to safely address unauthorized drone activity.
      - Develop and deploy advanced jammer-based mitigation that is effective against single drones as well as drone swarms (defined as

more than one drone) and sustainable as the threat seen around the world evolves in the U.S.

Thank you again for the opportunity to testify and I look forward to answering any questions you may have.