House Homeland Security Committee Joint Hearing

Subcommittee on Border Security and Enforcement and Subcommittee on Oversight Investigations and Accountability

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

Statement of David J. Berteau

President and CEO, The Professional Services Council

July 9, 2024

Introduction

Chairman Higgins, Chairman Bishop, Ranking Member Correa, Ranking Member Ivey and Members of the Committee, thank you for the invitation to testify on the role of technology and innovation in our nation's border security strategy.

I appear before you today on behalf of the Professional Services Council (PSC). We are a trade association of companies that do business with the federal government, with more than 400 member companies and hundreds of thousands of employees across the nation. PSC represents the full scope of the government contracting sector, with companies of all sizes (small, mid-sized, and large). Our member companies work in partnership with every cabinet department and agency, supporting every mission and function of the federal government.

I am here not just as the head of PSC but also as a person with more than 40 years of experience on these issues from all sides, including two stints inside the Pentagon as well as with industry, at a think tank, in academia, and now in my ninth year at PSC. I have run contracts that undertake to bring technology to border security and to the broader challenges of national security and addressing the government's needs. I have worked with state and local governments in partnership with Washington. I have seen the challenges that both sides face, and I have worked to provide what is needed to improve acquisition outcomes. In particular, I have long wrestled with how federal agencies can find, acquire, and use new technology and innovative processes and systems.

PSC's member companies provide the full range of technology and professional services to all federal agencies that pertain to our air, land, and sea border-related issues. Within the Department of Homeland Security, their customers include Customs and Border Protection (CBP), the U.S. Coast Guard (USCG), the Transportation Security Administration (TSA), and Immigration and Customs Enforcement (ICE). They also support agencies beyond DHS, including for example the Office of Refugee Resettlement (ORR) in the Department of Health and Human Services and the Justice Department's Executive Office for Immigration Review (EOIR) as well as many other programs and agencies.

PSC member companies help the government acquire and use multiple technologies, including detection systems, communication systems and networks, artificial intelligence and data

analytics, UAS (unmanned aerial systems) and counter-UAS, case management, information technology systems and infrastructure, and many other vital and emerging technologies needed for border security.

The diversity of contracts and customers, the range of solutions provided, and the size and reach of PSC member companies give us broad and deep perspectives on the challenges involved with identifying, procuring, and implementing technology and innovation to secure our borders and the important partnership role that our members and all of industry has in supporting border security in all its dimensions.

In Fiscal Year 2023 (FY23), DHS obligated more than $25 billion on contracts, including:

- $7 billion for CBP,
- $2 billion for TSA,
- more than $3 billion for ICE, and
- $1.4 billion for USCIS.

Both new and legacy technology needs make up a significant part of those contract dollars, playing essential and critical roles in protecting and securing the border. These contracts represent the partnership of government and industry, working together on the same goal – to develop and acquire the capabilities needed for mission success through systems and processes that are timely, cost effective, and accountable. That partnership operates within federal acquisition rules and regulations that encourage competition, innovation, and investment in the homeland security marketplace.

PSC Goals for the Government-Contractor Partnership Supporting Technology and Innovation

At PSC, we support this government-contractor partnership by focusing on three goals:

- making the government a smarter customer and a better buyer (i.e., knowing what to buy and how to buy it),
- improving contracting procedures to support technology modernization and innovation, and
- supporting policies and practices that build and sustain the workforces needed to meet government missions, both for our member companies and for their government customers.

First is to help the government become a smarter customer and a better buyer, leading to improved acquisition outcomes. Being a smarter customer means knowing what is available from every source, including the private sector, the national economy, and around the world. Being a better buyer means that, once the government identifies a product or service they can use, being better able to get the funds and procure that product or service. Both goals need to focus on getting better results for the government, consistent with its needs.

Second is to support technology modernization and innovation through contracts. The government is not alone in being able to find and get innovation and new technology. Contractors can and do play vital roles in extending the government's reach, capability, and capacity. I will have more to say on these vital roles later in this statement.

Third is to support workforces needed to meet government missions, both for our member companies and for their government customers. Better and more relevant training is an important part of workforce development and retention, and it is one of the areas that government contractors can strongly support. These goals are particularly important in all the areas affected by border security, where shortages of trained, experienced personnel is a long-standing issue.

In summary, the overall goal of PSC and our member companies is to help the government operate better, improve outcomes and results, and achieve its missions. These goals are particularly important in all aspects of achieving border security.

Keys to a Comprehensive and Successful Strategy

Next, I want to touch on the elements of a successful border security strategy. My Pentagon experience taught me that a successful strategy needs to address ends, ways, and means. Most importantly, a strategy is only as good as its implementation. A key element of successful implementation is for the strategy to include finding and using technology and innovation to support its goals.

"Ends" are the objectives, both as a final state and as the strategy is being followed. What are the goals?

"Ways" are the actions and reactions taken to pursue the strategy's objectives. What do you do, and particularly what do you do *differently*?

"Means" are the resources needed: the people, the equipment, the funds, the support, and the innovation and technology.

In essence, a strategy is a detailed plan, with goals, planned actions, and resources. Designing, issuing, and implementing any strategy, including a border security strategy, is a joint responsibility of the Congress and the executive branch, but it also depends on that government-industry partnership. Let me highlight some of the roles contractors play in setting and implementing strategy.

Our member companies do not develop or promulgate the government's strategies. They do not set the goals and objectives. Setting goals and defining the objectives (the "ends") of any strategy is the government's job, what the Office of Management and Budget calls "inherently governmental functions."

It is also the government's job to lay out the actions and reactions taken to pursue the strategy's objectives, the "ways" of the strategy.

The "means" are also set partially by the government. Executive branch agencies set up the offices and programs and, through the Congress, secure the funding, part of the "ways" of the strategy.

Where contractors come in is providing some of the rest of the "means," including the necessary people, equipment, facilities, and support. Throughout the implementation of a strategy, adjustments will be needed. On the border, for example, closing one access point might lead to increased use of another access point, requiring shifts in resources and activities. It is in that adjustment and adaptation where technology and innovation can play a big role, and contractors

are also the broadest and deepest source of technology and innovation to help that adjustment. Let's look at that more closely.

Technology and Innovation

At PSC, we connect the words "technology" and "innovation" to focus on ***technology*** solutions and ***innovation*** in systems and processes. Innovations can be changes in operations, improvements in integrating data, upgrading communications systems and networks, or cutting the time needed for a specific action. Often, the two (technology and innovation) go together. Incorporating a new technology can require, for example, changes in procedures, updates in training, or alternate ways to exchange data or to communicate.

Recent years have seen a call in the government for more innovation. This includes greater access to companies in the private sector, including companies with no prior federal government business. That approach should be part of the government's pursuit of innovation, but it's not enough. The government also needs to improve its use of ***today's*** contractors as a path to greater use of technology and innovation.

Why is that? It is because doing business with the federal government is not the same as doing business in the commercial market. Contractors are funded with taxpayer dollars, and the American public expects tighter, more rigorous government rules and regulations for federal contractors than for other private sector companies. Congress regularly responds to instances of contractor misconduct by updating or expanding laws that flow through those regulations.

These rules mean that companies that do business with the federal government must comply with myriad requirements and produce reports that depend on accounting systems, billing processes, employee timekeeping, and detailed information far beyond those needed for commercial business. The government often requires contractors to provide access to their proprietary intellectual property, their software code, or their trade secrets.

All of these compliance requirements are designed to support government goals, but they often contribute little to actually delivering results under a contract. In general, purely commercial companies do not need or have the systems and processes in place to certify compliance with government contracting requirements. Since failure to comply often can incur civil and criminal penalties and even result in a company being debarred from future government contracts, these rules add costs and time and are therefore a disincentive for commercial companies to compete.

Since existing government contractors already have those compliance systems in place, they are in a better position to help their government customers identify useful new technology and innovation and to work with the government to modify existing contracts to incorporate that new technology into delivering better results. Using existing contractors to identify and incorporate technology and innovation can reduce the risk for the government, help target new technology and innovation to those aspects of the mission where they will produce the greatest benefit, and provide improvements without the time-consuming effort to award new contracts.

The bottom line, then, is that both new and existing contractors can help the government incorporate technology and innovation to meet mission needs, including border security.

A Multi-Layered Border Security Strategy

A multi-layered border security strategy needs to include the necessary ends, ways, and means of any good strategy. But what would a multi-layered border security strategy need to cover?

It's critical to address the immediate zone of border crossings (detection, identification, interception, etc., both at or away from authorized ports of entry) of both the southern and northern borders as well as coastlines and airports, but a multi-layered strategy is more useful if it covers additional topics, including but not limited to, for example:

- U.S. needs for better intelligence before individuals arrive at any border
- entry points that are not at the land boundaries of the nation (air, sea)
- drugs or other unwanted materiel arriving in small packages or in containers (or via drones)
- tracking people, processing cases, and managing and reducing case backlogs
- detention, housing and medical care, etc., of individuals

This broader, multi-layered approach would involve more than CBP to include not only the relevant agencies and components of the federal government but also state and local governments and other nations. In all of these interactions, a multi-layered strategy would be better to the extent it incorporates new technology and innovation in products, systems, and processes, leading to better success across the broad definition of "border security."

Most importantly, for border security, a multi-layered strategy needs to be more than simply "ends, ways, and means." The actions (the "ways") and the resources (the "means") need to be integrated, tied together in a common operating picture and interoperable, accessible, and useable by all players. Doing that demands better use of new technology and innovation across the board.

Why Is It Hard For the U.S. Government To Use Technology and Innovation?

It is hard to get the government to see the value of new technology, new systems, and new processes, to allocate scarce funds to buy and use them, and to change how it operates so that it can realize the advantages of that innovation. Why is this so hard? Here is what I've learned.

1) It is hard for the government to identify or become aware of applicable and relevant new technology, systems, and processes;

2) It takes time (years) to plan, program, budget, and get Congress to provide the necessary funding to procure and use technology and innovation;

3) It takes more time to solicit, evaluate, and award the contracts or buy the technology; and

4) It takes still more time to get the government personnel at all levels to deploy and use the new systems and processes and technology.

Using existing contractors, as noted above, can cut some time from these steps, but it still takes too long.

What, then, do we suggest will address all the issues outlined above?

PSC Suggestions To Improve Access to and Use of Technology and Innovation

PSC draws on the experiences of its member companies as they undertake to identify innovations and new technology, offer them to the government, and incorporate them into ongoing operations. Based on that, we offer the following suggestions as ways to improve access to and use of technology and innovation.

1) Earlier and More Comprehensive Identification of Innovations and Technology for Border Security

DHS components can improve their ability to find useful technology and systems and process improvements through actions such as:

- Focus their requirements, both for contracts and for operations, on results and outcomes, not just on inputs, and promulgate those requirements publicly so that companies can work to develop technology to meet them. Update the requirements often to incorporate available innovation.

- Develop and make publicly available a long-term (e.g., five year) investment plan and update that plan regularly.

- Expand communications with industry and encourage both existing and potentially new contractors to offer solutions. Give feedback to those offerings.

2) Support Long-Term Resource Commitments and Increase Flexibility for Existing Resources

DHS can improve its use of existing funding and justify the need for additional funding. These suggested steps and improvements may help.

- Border security will be substantially improved if Congress appropriates funds on time, by the beginning of the fiscal year, avoiding continuing resolutions or the disruptive threats of a government shutdown. On-time appropriations will enable DHS components to access technology and innovation faster and get results sooner.

- DHS can use existing reprogramming authority earlier and more often in the fiscal year to address emerging needs and opportunities. (Note that this needs support from both the White House and Congress.)

- Use multi-year funding and contracts to support key investments in new technology.

3) Speed Contract Awards

An age-old problem with the government is that, when contracts take too long to put in place, by the time new technology is procured, it will no longer be new. Recent data show clearly that, across the government, the time between a contract solicitation and the award of that contract has been getting longer. In addition, delays appear to be increasing in the period of time before a solicitation is issued. Both of these problems need attention by DHS and Congress.

Congress can help by conducting oversight hearings that illuminate both the increased time consumed by contracting and the causes and possible fixes to reduce that time. Congress can also help by requiring annual reports from DHS on procurement and administrative lead times for all types and sizes of contracts.

4) Training To Use New Technology

We all know how hard it is to adapt to an upgrade or an innovation in something that we are used to, whether it's using a new cell phone, the latest version of the operating system of a laptop, or the features and controls of a new car. This same dynamic exists when any agency or component incorporates new technology and innovation into existing operations.

To offset this natural occurrence, DHS components could plan for and fund the time, the resources, and the capacity and capability to train the workforce to take advantage of new technology. Contractors can help develop and provide that training more rapidly and broadly.

Conclusion

In closing, on behalf of PSC and our members, I thank you for your time and consideration of these matters. PSC member companies are proud to work with CBP, with DHS, and with other federal departments and agencies to provide technology and increase innovation for border security. We are committed to the missions.

As always, PSC is available at your convenience to address any questions or concerns the Committee has, now and in the future. I will try today and for the record to answer any questions you may have, and I look forward to continuing to work with the Committee and these Subcommittees on these issues. Thank you.

TESTIMONY OF

Thaddeus C. Cleveland
Sheriff
Terrell County, Texas

For a Hearing

BEFORE

U.S. House of Representatives
Committee on Homeland Security

ON

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

July 9, 2024
Washington, DC

Chairman Green, Ranking Member Thompson, Distinguished Members of the Committee, thank you for the opportunity to discuss the conditions along the Southwest Border and the efforts by the Terrell County, Texas, Sheriff's Office to serve and protect our citizens.

I am honored to represent the citizens of Terrell County and describe to you what the citizens, law enforcement, and Border Patrol experience in our portion of the United States and Mexico border.

Other than my time in the United States Air Force and in Washington, D.C., while assigned to U.S. Border Patrol Headquarters, I've spent my entire life as a resident and in the U.S. Border Patrol along the U.S./Mexico border. The last 11 years of my 26-year Border Patrol career were spent as the Patrol Agent in Charge of the Sanderson Border Patrol Station, which is also my hometown and where I am Sheriff.

As background, Terrell County is located in the rugged, unforgiving, vast Big Bend Region of Texas and shares 54 miles of international border with Mexico. Terrell County is the 10th largest county in the State of Texas and encompasses almost 2,400 square miles. The Border Patrol Station there is responsible for 91 miles of border, which is the third largest portion of border with Mexico by a United State Border Patrol Station along the entire U.S./Mexico border.

Terrell County, does not have a crime problem, we have is a Border Security problem. Over the last 3 ½ years, Terrell County like much of the Southwest Border has seen a significant increase in illegal alien apprehensions; however, what has happened in Eagle Pass, Del Rio, El Paso, Lukeville and San Diego with masses of people crossing the border, does not happen in Terrell County. What we experience are people who do not want to be apprehended nor give-up. When we encounter them in the desert, they run. When we encounter them on the highways, they lead us in high-speed pursuits before bailing out and absconding.

The next set of statistics I am going to share with you are the Sanderson Border Patrol Station fiscal year apprehension and gotaway percentages compared to fiscal year 2020. In fiscal year 2021 there was a 289% increase in illegal alien arrests and a 323% increase in gotaways. In fiscal year 2022, there was a 417% increase in illegal alien arrests and a 467% increase in gotaways. Last fiscal year, there was a decrease in apprehensions and gotaways, but it was still

higher than the historical numbers with 189% increase in illegal alien arrests and 203% gotaways.

Citizens of Terrell County pay the price daily for the out-of-control Southwest Border. We do not have the financial, medical or emergency resources as many of the other larger communities affected by the activity along the border. Yet, the negative and detrimental results are the same. Valuable and costly emergency and medical resources are too often diverted to border security. In my county, landowners have to repair waterlines, fences and structures destroyed by illegal aliens crossing their properties, as well as the significant trash, human biohazard waste and erosion. Emergency medical services and law enforcement service has at times been unavailable due to responding to illegal aliens that are crossing the border.

There has been a total of 37 known deaths of illegal aliens attempting to cross my portion of the border over the last the 3 ½ years. Historically, there was one a year. All but four of those deaths were from exposure due to the hot summer months as well as the cold winter fronts that come through Terrell County. Four died in a vehicle pursuit, which resulted in a head-on collision. High-speed pursuits occur with almost every illegal alien smuggling load encountered and puts citizens my team and I are responsible for in harm's way.

Due to the amount of illegal alien smuggling activity coupled with the amount of vehicle pursuits we were involved in since I took over as Sheriff, I reached out to Governor Abbott of the State of Texas and requested additional resources to assist my office. Governor Abbott and I discussed the situation, and within a week, the additional resources I requested were allotted. With assistance from the Texas Department of Public Safety and Texas Parks and Wildlife, together we seized over 100 vehicles from illegal alien smugglers in the months of November 2022. Since then, we have observed a shift in tactics by smugglers and are not seeing the same level of activity in Terrell County. Those shifts in tactics is what brings us together today to discuss technology and advancements.

I have seen the U.S. Border Patrol evolve with technology. Technological evolutions have assisted the U.S. Border Patrol achieve tremendous success with border security. I've witnessed seismic and magnetic sensors evolve into imaging sensors, scope trucks have evolved from

black blobs on a screen to Mobile Video Surveillance Systems, which use infrared night vision and radars with a near crystal clear view.

As the Patrol Agent in Charge of the Sanderson Border Patrol Station, I worked with Sheriff Ronny Dodson of Brewster County, former Terrell County Sheriff Clint McDonald to develop a network of Buckeye game cameras that shared real-time images to our respective offices. This was a collaborative effort to enhance border security and was the first effort of its kind along the U.S./Mexico border.

Also, during my command of the Border Patrol Station in Sanderson, Texas, we received and deployed our first eight Autonomous Surveillance Towers. This is an incredible asset, yet we quickly learned they detected more activity and we did not have the manpower to pursue everything the towers revealed. With that being said, you can have as much technology on the border, but without the right balance of manpower, the technology is useless.

The State of Texas is also utilizing various technology platforms along the U.S./Mexico border. In 2008, I was assigned as U.S. Border Patrol's representative to the State of Texas, during this time, Texas Department of Public Safety first deployed their Drawbridge game cameras along the along the U.S./Mexico border. This program now has over 7,000 game cameras along the border. The State of Texas has also constructed over 40 miles of border wall in Texas and has mounted camaras systems on the wall as well.

As Sheriff, through Operation Lone Star, my office has been able to receive night vision and thermal imaging devices and we are waiting on approval of three Mobile Video Surveillance platforms.

I think defining success for border security initiatives at the county level involves a collaborative approach and setting realistic, localized objectives. Success at the county level is measured by our ability to effectively utilize limited resources to enhance security and reduce illegal activity. This means fostering strong partnerships with federal and state agencies, maximizing the impact of every dollar spent, and ensuring our personnel are well-trained and equipped.

One key indicator of success has been our effective use of grants and state programs. For example, through Operation Lone Star and Operation Stone Garden, we've been able to hire additional deputies, acquire new vehicles, and obtain vital technology like thermal cameras and night vision equipment. These resources have significantly bolstered our capability to patrol and secure the border.

Our success is also evident in the reduced level of illegal activity in Terrell County. By taking control of the highways and leveraging surveillance technology, we've deterred illegal crossings and forced smugglers to reroute further north, avoiding our jurisdiction. This shift is confirmed through intelligence reports and feedback from sources on the ground.

At the federal level, success is often measured by broader metrics, such as overall apprehension numbers and the implementation of large-scale infrastructure projects. The federal government operates with a much larger budget and a focus on nationwide border security strategies. In contrast, at the county level, we work with more constrained budgets and focus on immediate, localized impacts.

Ultimately, success for us is defined by our ability to protect our community efficiently and effectively, using available resources and strong partnerships to fill gaps where federal and state support is limited. This local perspective ensures that we address specific threats and challenges unique to our region, contributing to the overall border security efforts in a meaningful way.

The chaos along our Southwest Border is solvable and preventable. Solutions exist, they need only ask those of us on the ground dealing with this every day. The border is open, overrun, and the criminal organizations are taking full advantage of our political gridlock.

To secure our borders we must go back to securing the areas in between our Ports of Entry. To do this, added resources such as manpower, technology and infrastructure are required to detect, track and apprehend those who mean us harm. Additionally, we must always be prepared for a mass migration crisis. We must bolster our current infrastructure to include the addition of more detention centers that are used for short and long-term detention of illegal aliens, that include immigration judges at each location to expedite immigration hearings.

Ports of Entry along the Southwest Border should be designated for specific needs such as political relief, natural disasters, and work-related industries.

Border Security and Immigration Reform are separate and individual issues. They should be kept and managed separately as border security does not just focus on illegal immigration. Border security is paramount to National security.

To ensure the security of our nation, those of us that have sworn an oath to protect and defend the Constitution of the United States must come together to develop, implement and execute viable solutions. This is why I am in speaking to you today. The advancement of technology has been key to securing America's border. Technology coupled with the ingenuity of Border Patrol Agents will continue to grow America's advancement of border security. Partnerships and leveraging technologies at the federal, state and local level is also necessary to keep American and American's protected.

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.

---

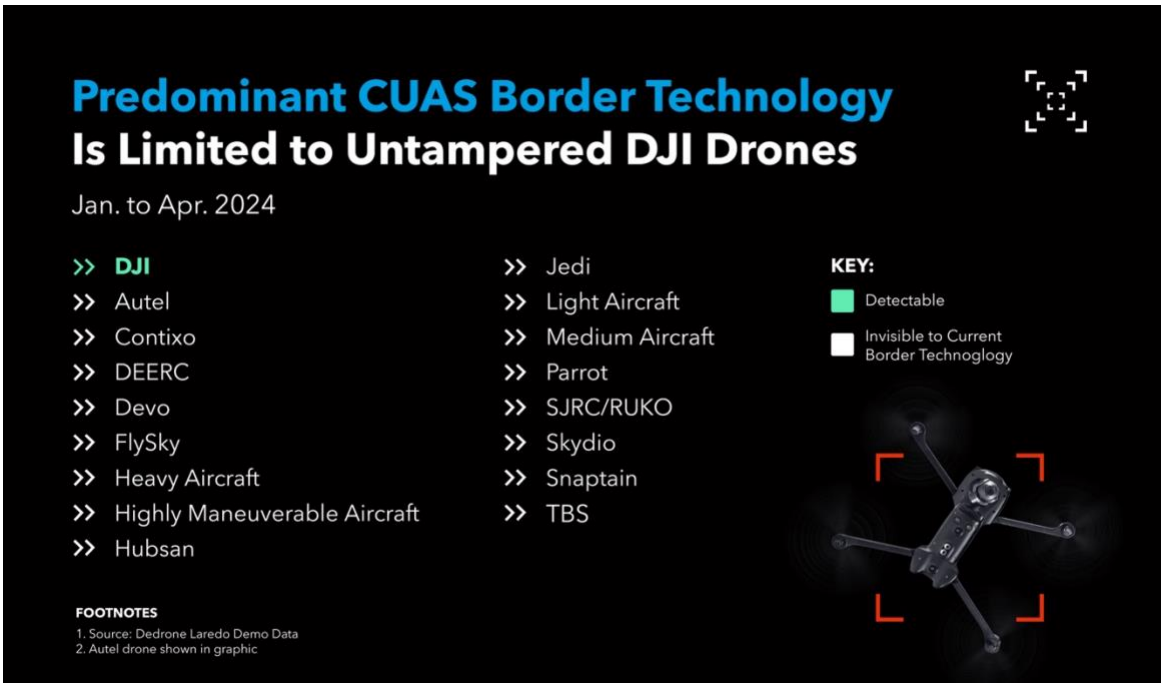
[1] Narcosis, *8 Arrested in Mexico For Manufacturing Drone Explosives*, ATLAS NEWS (Oct. 9, 2023).
[2] *CJNG attack against indigenous community of Michoacán denounced*, EJECENTRAL (Jul. 4, 2024).
Mark Stevenson, *Mexican cartels now use IEDs as well as bomb-dropping drones*, ASSOCIATED PRESS (Feb. 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

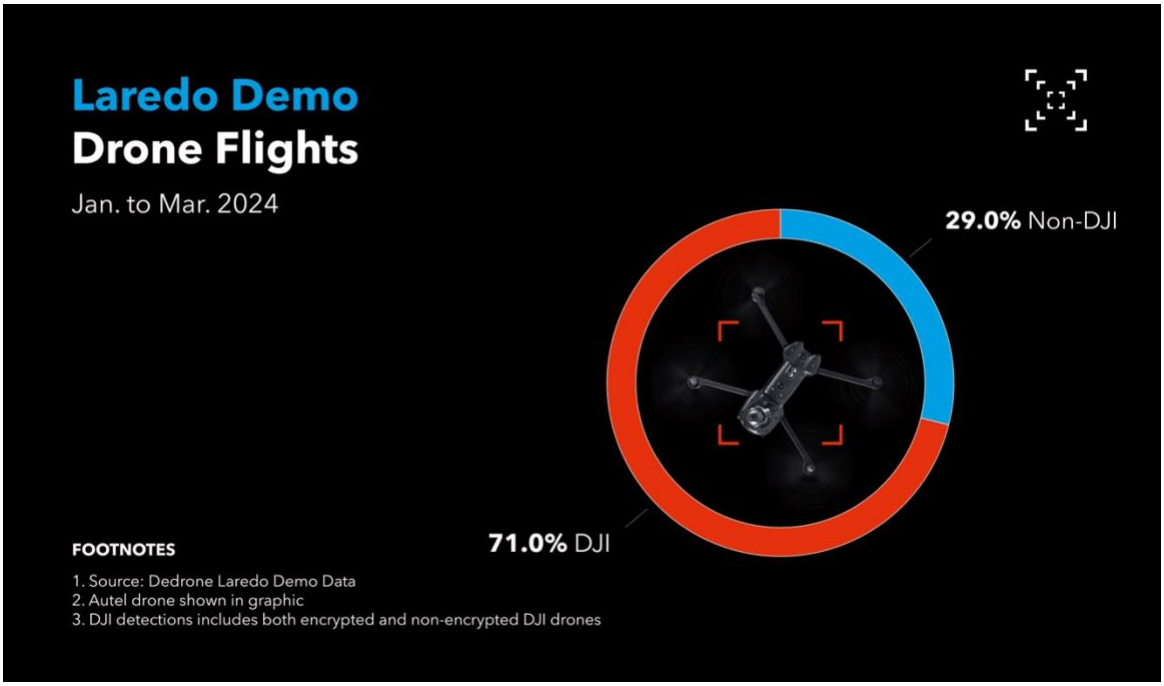
In January of this year, Dedrone entered into an official contract with CBP – at no cost to the government – to perform a demonstration project of C-UAS capabilities along a five-mile stretch of the U.S.-Mexico border in Laredo, TX. To date, Dedrone has invested over $3.3 million to establish full spectrum 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.